MISSISSIPPI LAW JOURNAL

Volume 78, Number 2 *Winter 2008*

SYMPOSIUM

THE FOURTH AMENDMENT AT THE INTERNATIONAL BORDER

SPONSORED BY THE
NATIONAL CENTER FOR JUSTICE AND THE RULE OF LAW

FOREWORD — *Thomas K. Clancy*

THE PUBLIC AND THE PRIVATE AT THE UNITED STATES BORDER WITH CYBERSPACE — *John Palfrey*

BORDER SEARCHES IN THE AGE OF TERRORISM — *Robert M. Bloom*

ELECTRONIC SURVEILLANCE AT THE VIRTUAL BORDER — *Susan Freiwald*

BORDER FICTION: DOES AN ANALOGY TO IMMIGRATION LAW ALLEVIATE FOURTH AMENDMENT ANXIETY? — *Matthew R. Hall*

COMBATING TERRORISM IN THE DIGITAL AGE: A CLASH OF DOCTRINES: THE FRONTIER OF SOVEREIGNTY—NATIONAL SECURITY AND CITIZENSHIP—THE FOURTH AMENDMENT—TECHNOLOGY AND SHIFTING LEGAL BORDERS — *Harvey Rishikof*

THE JAMES OTIS LECTURES

INTRODUCTION TO JAMES OTIS LECTURES — *Thomas K. Clancy*

ENVISIONING POST-CONVICTION REVIEW FOR THE TWENTY-FIRST CENTURY — *Nancy J. King and Joseph L. Hoffmann*

Digitized by the Internet Archive
in 2012 with funding from
LYRASIS Members and Sloan Foundation

http://archive.org/details/mississippilawjo78thom

MISSISSIPPI LAW JOURNAL
109 LAMAR LAW CENTER, ROOM 111
UNIVERSITY MS 38677

ADDRESS SERVICE REQUESTED

NON PROFIT ORGANIZATION
US POSTAGE PAID
LINCOLN NE
PERMIT NO 264

64

BROWN, RAYMOND
BROWN-BUCHANAN-SESSOMS, PA
P.O. BOX 2220
PASCAGOULA MS 39569-2220

PRINTED MATTER BOOKS

Become a Friend of the *Mississippi Law Journal*

Today the *Mississippi Law Journal* is funded and operated almost exclusively through student efforts. Increasingly, however, the *Journal* depends on the support of its alumni and friends. You can become a Friend of the *Mississippi Law Journal* by making a tax-deductible contribution to one of the funds listed below. Checks should be made payable to the University of Mississippi Foundation and mailed to Post Office Box 8288, University, Mississippi 38677. *Please indicate on your check to which fund you intend to contribute.*

Robert C. Khayat Scholarship Endowment

The Robert C. Khayat Scholarship Endowment was established in 1995 to honor the dedicated service of Robert C. Khayat, a *Journal* alumnus, professor of law, and current Chancellor of the University. Each year the *Journal* awards the Robert C. Khayat scholarship to a deserving member.

As of June 30, 2007, the corpus of the endowment was $81,696.18. Last year the *Journal* awarded a scholarship in the amount of $1,000.00. The *Journal* intends to award larger scholarships as the corpus grows.

Mississippi Law Journal Endowment

The *Mississippi Law Journal* Endowment exists to ensure the *Journal*'s future financial stability. As of June 30, 2007, the corpus of the endowment was $349,114.08.

Mississippi Law Journal Operating Fund

All contributions to the *Mississippi Law Journal*'s operating fund help the *Journal* to meet its most immediate needs, including office maintenance.

Friends of the *Mississippi Law Journal**

Dr. Guthrie T. Abbott
Mrs. Paula Graves Ardelean
The Honorable Rhesa H. Barksdale
Mr. Ross F. Bass
Mr. William H. Beck Jr.
Bennett Lotterhos Sulser and Wilson
The Honorable William H. Bizzell
The Honorable Eugene M. Bogen
Mrs. Teri M. Bowie
Mrs. Lorraine Walters Boykin
Mr. John R. Braley IV
Mr. Charles L. Brocato
Mr. Lampkin Herbert Butts Sr.
Mr. James T. Caldwell
The Honorable Thad Cochran
Mr. Richard G. Cowart
Mr. T. David Cowart
Mr. Frank Crosthwait
Mr. Joseph Dale
Mr. William M. Deavours
Mrs. Marlane Dove
Mr. W. W. Drinkwater Jr.
Dulin & Dulin Ltd.
Lt. Commander W.J. Dunaway
Dr. Wylene W. Dunbar
Mr. Richard M. Edmonson Sr.
Mr. Herbert C. Ehrhardt
Dr. Martha Jane Ellis
Mr. Roger M. Flynt Jr.
Mr. William M. Gage
Mr. Robert C. Galloway
Mrs. Gretchen L. Gentry
Mr. Eugene B. Gifford Jr.
Mr. Hampton Glover Jr.
Mr. William N. Graham
Mr. Newt P. Harrison
Mr. Robert H. Hodges
Mr. Jamie G. Houston III
Mr. Gary K. Jones
Mr. W.R. Jones Jr.
Mr. William T. Jones
Mrs. Patricia Fleming Kennedy
Mr. William N. Krucks
The Honorable Tom Stewart Lee
Mrs. Virginia C. Lococo
Mr. Roland Marble Sr.
Mr. M.C. Maxwell
Ms. Lydia H. McIntosh
Mr. Jason N. McNeel
Mr. Joseph R. Meadows

Michael T. Lewis
Mr. Russell W. Mills
Mr. David W. Mockbee
Mr. H. Dixon Montague
Mr. Dalton M. Mounger
Mrs. Julie Sneed Muller
Mr. Christopher Tyson Nettles
Mr. James W. O'Mara
The Honorable J. D. Orlansky
Mr. Tom Ostenson
Mr. James A. Peden Jr.
Mr. Leroy D. Percy
Mr. Richard T. Phillips
Mr. Rubel L. Phillips
Mr. Benjamin J. Piazza Jr.
Mr. George B. Pickett Jr.
Mr. C. Michael Pumphrey
Mr. Clayton C. Purdom
Mr. Holloman M. Raney
Mr. Eric Tyson Ray
Mr. Richard Roberts III
Mr. Lucius F. Sams Jr.
Ms. Lillous A. Shoemaker
Mr. George M. Simmerman Jr.
Mr. Jimmy Sledge Jr.
The Honorable Elzy J. Smith Jr.
Mr. W. Marion Smith
Mr. Ronald T. Solberg
Mr. Darrell Solomon
Mr. Arthur D. Spratlin Jr.
Mrs. Patricia L. Stevens
Mr. Phineas Stevens
Mr. Samuel James Stigler
Mrs. Molly Fergusson Stuart
Mrs. Nancy H. Stumberg
Ms. Margaret J. Murphy Sweetland
Mr. Frank W. Trapp
Mr. Clint Douglas Vanderver
Mr. J. P. Varner
Mr. Lawrence D. Wade
Mrs. Michelle Clingan Waits
Mr. Tim Walsh
Mr. George D. Warner Jr.
Mr. Irwin G. Waterman
Mr. Louis H. Watson Jr.
Mr. Walker L. Watters
Dr. Robert A. Weems
Mr. John T. Wilkinson Jr.
Mr. Eddie C. Williams

** As of December 15, 2008*

The *Mississippi Law Journal* is published four times during the school year. The *Journal*'s editorial and business offices may be contacted via U.S. mail at: Post Office Box 849, University, Mississippi 38677.

Manuscripts: Manuscripts should be submitted electronically to **misslj@olemiss.edu**. Manuscripts should be in 12-point type and double-spaced, in Microsoft Word, WordPerfect, or PDF. Citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (18th ed. 2005).

Subscriptions: $35.00 per year. Single issue: $12.00. Subscriptions are renewed automatically upon expiration unless the subscriber sends a notice of termination.

Change of address: Send address changes directly to the *Mississippi Law Journal*. Include name, new address (including zip code) and old address. Please notify the *Journal* forty-five days in advance to ensure prompt delivery.

Back Issues: Back issues of the *Mississippi Law Journal* may be ordered directly from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York 14029-1987. Orders may also be placed by calling William S. Hein & Co., Inc., at (800) 828-7571, via fax at (716) 883-8100 or email to order@wshein.com. Back issues are available in PDF format through HeinOnline.

The *Mississippi Law Journal* is a member of the National Conference of Law Reviews. To offer its contributors complete freedom, the *Journal* assumes no responsibility for the views expressed herein.

Mississippi Law Journal

Published by Students at
The University of Mississippi School of Law

VOLUME 78 **Winter 2008** **NUMBER 2**

Copyright © 2008, Mississippi Law Journal, Inc.

Editor-in-Chief
SUSANNA T. MOORE

Executive Editor
E. DAN MARTIN

Articles Editors
BLAKE ADAMS
NAKIMULI DAVIS
GRETCHEN J. HARRIS

Business Manager
KAP PRIMOS

Notes & Comments Editor
KACY MCCAFFREY

Mississippi Cases Editor
NICK THOMPSON

ASSOCIATE EDITORS

Articles Editors
KATE MURPHY BOGARD
BETH BRYANT
MEREDITH EDWARDS
JOHN GRANT
JENNIFER HERRING
MARI KLEVEN
BRANT RYAN
JUSTIN STARLING
LINDSEY SMITH WISEMAN

Developmental Editors
ALSTON LUDWIG
BLAKE SMITH

Faculty Advisors
DEBORAH H. BELL
JOHN CZARNETZKY
ROBERT A. WEEMS

Mississippi Cases Editors
JENESSA CARTER HICKS
LAUREN HILLERY
JARED MARTIN
LINDSAY MURPHY

Managing Editor
JASON A. CROOK

Notes & Comments Editors
WILL BEASLEY
PRICE DONAHOO
NICHOLAS GREENE

Membership Director
JONATHAN COBB

Office Manager
JAMES HALTOM

STAFF

Catherine E. Ashburn
Cody C. Bailey
Allison Barrett
Bette Killebrew Bradley
Preston Burford
Drew Compton
Padrick D. Dennis
Shelly Mott Diaz
William J. Dukes
Julie C. Ely
Steven Griffin
John Helbling
Julie L. Howell
Lori Johnson
Mike Jones
D. Sterling Kidd
E. Richardson LaBruce
Jenna N. Leet
J. Scott Magee
Leontra Mayes
Kelly McReynolds
Kristie L. Metcalfe
Bill Nichol
Arthur J. Park
Amanda Proctor
Trevor B. Rockstad
Bradley Smith
Daniel Stephenson
Nicholas D. Welly
Steven Woodliff

Administrative Officers of the University of Mississippi

ROBERT C. KHAYAT	*Chancellor*
MORRIS H. STOCKS	*Interim Provost and Vice Chancellor for Academic Affairs*
GLORIA KELLUM	*Vice Chancellor for University Affairs*
ALICE CLARK	*Vice Chancellor for Research and Sponsored Programs*
LARRY SPARKS	*Vice Chancellor for Administration and Finance*
WENDELL WEAKLEY	*President/CEO, The University of Mississippi Foundation*
THOMAS WALLACE	*Assistant Provost*
ANDREW P. MULLINS, JR.	*Executive Assistant to the Chancellor*
TIMOTHY L. WALSH	*Executive Director of Alumni Affairs*
SAMUEL M. DAVIS	*Dean of the School of Law, Director of Law Center, Jamie L. Whitten Chair of Law and Government and Professor of Law*

THE LAW SCHOOL FACULTY

GUTHRIE T. ABBOTT, *Professor Emeritus and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law Emeritus*

MICHELE ALEXANDRE, *Assistant Professor of Law*

RICHARD L. BARNES, *Professor of Law and Leonard B. Melvin, Jr. Distinguished Lecturer in Law*

DEBORAH H. BELL, *Professor of Law, Mississippi Defense Lawyers Association Distinguished Lecturer and Director of the Civil Legal Clinic*

WILLIAM W. BERRY, III, *Visiting Assistant Professor of Law*

P.J. BLOUNT, *Research Counsel and Instructor*

JOHN R. BRADLEY, *Professor of Law*

PHILLIP W. BROADHEAD, *Director, Clinical Appeals Program and Clinical Professor of Law*

CHARLES BROWER, II, *Croft Associate Professor of International Law and Jessie D. Puckett, Jr. Lecturer in Law*

MERCER E. BULLARD, *Associate Professor of Law*

LARRY BUSH, *Professor Emeritus of Law*

W. TUCKER CARRINGTON, *Director, Mississippi Innocence Project*

DAVID W. CASE, *Associate Professor of Law*

BENJAMIN P. COOPER, *Assistant Professor of Law*

WILLIAM M. CHAMPION, *Professor Emeritus and Mississippi Defense Lawyers Association Distinguished Lecturer Emeritus*

THOMAS K. CLANCY, *Director of the National Center for Justice and the Rule of Law and Research Professor of Law*

GEORGE C. COCHRAN, *Professor of Law*

AARON S. CONDON, *Professor Emeritus of Law*

JOHN M. CZARNETZKY, *Professor of Law and Mitchell, McNutt, and Sams Lecturer*

DONNA DAVIS, *Associate Professor of Law*

JASON DERRICK, *Acting Assistant Professor of Legal Writing*

KYLE DUNCAN, *Assistant Professor of Law*

THOMAS R. ETHRIDGE, *Professor Emeritus of Law*

D. MICHAEL FEATHERSTONE, *Professor Emeritus of Law*

MOLLY FERGUSSON, *Acting Assistant Professor of Legal Writing*

DON L. FRUGE, *Professor Emeritus and President and CEO Emeritus of the University of Mississippi Foundation*

JOANNE I. GABRYNOWICZ, *Director of the National Remote Sensing, Air and Space Law Center and Research Professor of Law*

KRIS L. GILLILAND, *Director of Law Library and Associate Professor of Law*

CHRISTOPHER GREEN, *Assistant Professor of Law*

KAREN O. GREEN, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*

MATTHEW R. HALL, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

MICHAEL H. HOFFHEIMER, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*

ROBERT C. KHAYAT, *Chancellor and Professor of Law*

PATRICIA KRUEGER, *Acting Assistant Professor of Legal Writing and Director of Academic Excellence Program*

DON MASON, *Associate Director of the National Center for Justice and the Rule of Law and Lecturer*

GARY MYERS, *Professor of Law and Ray and Louise Stewart Lecturer*

JACK W. NOWLIN, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

E. FARISH PERCY, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

LARRY J. PITTMAN, *Professor of Law and Jessie D. Puckett, Jr., Lecturer*

LISA S. ROY, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

RONALD J. RYCHLAK, *Associate Dean for Academic Affairs, Professor of Law and Mississippi Defense Lawyers Association Lecturer*

JACQUELINE SERRAO, *Associate Director of the National Remote Sensing, Air and Space Law Center*

HANS P. SINHA, *Director of Prosecutorial Externship Program and Clinical Professor of Law*

CAROLYN ELLIS STATON, *Special Asssistant to the Chancellor and Professor of Law*

ROBERT A. WEEMS, *Professor of Law and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law*

C. JACKSON WILLIAMS, *Director of Legal Writing Program and Acting Assistant Professor of Legal Writing*

Mississippi Law Journal

Published by Students at
The University of Mississippi School of Law

VOLUME 78 **Winter 2008** **NUMBER 2**

Copyright © 2008, Mississippi Law Journal, Inc.

TABLE OF CONTENTS

SYMPOSIUM

THE FOURTH AMENDMENT AT THE INTERNATIONAL BORDER

Sponsored by the
National Center for Justice and the Rule of Law

FOREWORD
..... *Thomas K. Clancy* i

THE PUBLIC AND THE PRIVATE AT THE UNITED STATES BORDER WITH CYBERSPACE
..... *John Palfrey* 241

BORDER SEARCHES IN THE AGE OF TERRORISM
..... *Robert M. Bloom* 295

ELECTRONIC SURVEILLANCE AT THE VIRTUAL BORDER
..... *Susan Freiwald* 329

BORDER FICTION: DOES AN ANALOGY TO IMMIGRATION LAW ALLEVIATE FOURTH AMENDMENT ANXIETY?
..... *Matthew R. Hall* 363

COMBATING TERRORISM IN THE DIGITAL AGE: A CLASH OF DOCTRINES: THE FRONTIER OF SOVEREIGNTY—NATIONAL SECURITY AND CITIZENSHIP—THE FOURTH AMENDMENT—TECHNOLOGY AND SHIFTING LEGAL BORDERS
..... *Harvey Rishikof* 381

THE JAMES OTIS LECTURES

INTRODUCTION TO JAMES OTIS LECTURES
..... *Thomas K. Clancy* 431

ENVISIONING POST-CONVICTION REVIEW FOR THE TWENTY-FIRST CENTURY
..... *Nancy J. King* and *Joseph L. Hoffmann* 433

FOREWORD
2008 FOURTH AMENDMENT SYMPOSIUM

THE FOURTH AMENDMENT AT THE INTERNATIONAL BORDER

*Thomas K. Clancy**

The National Center for Justice and the Rule of Law,[1] which is a program of The University of Mississippi School of Law, focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. In furtherance of its mission, the Center has established the *Fourth Amendment Initiative.* The purpose of the Center's initiative is to promote awareness of Fourth Amendment principles through conferences, publications, and training of professionals in the criminal justice system. The Center takes no point of view as to the direction that Fourth Amendment analysis should take but seeks to facilitate awareness of the issues and encourage discussion of search and

* Director, National Center for Justice and the Rule of Law, and Research Professor, The University of Mississippi School of Law.

[1] The National Center for Justice and the Rule of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles stemming from this symposium are those of the author and do not represent the official position of the United States Department of Justice. For more information about the Center, please visit www.ncjrl.org.

seizure principles.

A central pillar of the *Fourth Amendment Initiative* is its annual symposium on important search and seizure topics. On April 15, 2008, the Center hosted its annual symposium, which coincided with the second day of a conference entitled *The Fourth Amendment: Contemporary Issues for Appellate Judges*, sponsored by the Center in cooperation with the National Judicial College. The Center believes that the symposium—and the insightful articles published in this special edition of the *Mississippi Law Journal* that stemmed from the presentations at that event—significantly further the Center's mission and, more importantly, make significant contributions to the understanding of search and seizure principles. The Center, and I personally, wish to thank the leading legal scholars who participated.

Five distinguished scholars spoke at the symposium and wrote articles for this edition of the law journal: Professor Robert Bloom, of Boston College Law School; Professor Susan A. Freiwald, of the University of San Francisco School of Law; Associate Professor Matthew Hall, of the University of Mississippi School of Law; Professor John Palfrey, Executive Director, Berkman Center for Internet and Society, at Harvard University School of Law; and Professor Harvey Rishikof, of the National War College. After providing an overview of the Supreme Court's border doctrine jurisprudence, each of their articles will be introduced.

OVERVIEW OF THE INTERNATIONAL BORDER DOCTRINE[2]

Travelers, their baggage, goods, and other items crossing the international border[3] of the United States are subject to

---

[2] This summary is largely drawn from THOMAS K. CLANCY, *THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION* § 10.2. (Carolina Academic Press 2008).

[3] The power to search and seize without suspicion extends to persons and goods leaving the country. *See generally* Larry Cunningham, *The Border Search Exception as Applied to Exit and Export Searches: A Global Conceptualization*, 26 QUINNIPIAC L. REV. 1 (2007). It also extends to the functional equivalent of the international border. *E.g.*, Almeida-Sanchez v. United States, 413 U.S. 266, 272-73 (1973). Border searches without suspicion may, under certain circumstances, include searches in the United States'

search.[4] This *sui generis* power is grounded on national sovereignty, that is, the federal government has both the right and obligation to protect the nation's borders from legally excludable persons and things.[5] That authority has strong historical roots.[6] There is language in the cases speaking of that

---

interior of those who have recently crossed the border, based on surveillance starting at the border. *E.g.*, United States v. Hill, 939 F.2d 934 (11th Cir. 1991). Congress has given the Coast Guard and customs officials broad authority to stop and seize on water. *See, e.g.*, United States v. Villamonte-Marquez, 462 U.S. 579 (1983) (individualized suspicion not required for Coast Guard or Customs Service to board vessel and to examine owner's documents in waters where vessel has ready access to open sea). Also, the Fourth Amendment is inapplicable to searches and seizures against aliens in international waters. United States v. Bravo, 489 F.3d 1, 8-9 (1st Cir. 2007). Attempts to protect national sovereignty have moved away from the immediate vicinity of the border and into areas appurtenant to it. Law enforcement efforts in such areas are not considered border searches, although the national interest in protecting against such activities as illegal immigration and smuggling have been viewed as weighty governmental interests. Several investigative techniques have been utilized by immigration authorities. Roving patrols by immigration authorities have been held to need articulable suspicion of criminal activity before stopping vehicles that are not known to have crossed the border, even though they are traveling near it. United States v. Brignoni-Ponce, 422 U.S. 873 (1975).

[4] *E.g.*, Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973); Carroll v. United States, 267 U.S. 132, 154 (1925). *See also* California Bankers Ass'n v. Shultz, 416 U.S. 21, 62-63 (1974) (upholding regulation requiring record keeping of certain international banking transactions). *Cf.* Von Cotzhausen v. Nazro, 107 U.S. 215, 218 (1883) ("all the vexatious and annoying machinery of the custom-house, and the vigilance of its officers, are imposed by law to prevent even the smallest evasion" of the revenue laws).

[5] *E.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 538-39 (1985) (emphasizing sovereignty interests at the border); Almeida-Sanchez v. United States, 413 U.S. 266, 291 (1973) (White, J., dissenting) ("Jurisdiction over its own territory . . . is an incident of every independent nation."); Carroll v. United States, 267 U.S. 132, 154 (1925) (speaking of the power of "national self-protection"); Boyd v. United States, 116 U.S. 616, 623 (1886) (acknowledging the long pedigree and constitutionality of customs searches and seizures). "At the border, customs officials have more than merely an investigative law enforcement role. They are also charged, along with immigration officials, with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." *Montoya de Hernandez*, 473 U.S. at 544.

[6] The power of customs officials to conduct searches at the border has an "impressive historical pedigree." United States v. Villamonte-Marquez, 462 U.S. 579, 585 (1983). "Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." United States v. Montoya de

power in absolutist terms: "The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity."[7] As another example, the Court has stated:

> Border searches . . . from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself.[8]

Most recently, the Court has stated:

Hernandez, 473 U.S. 531, 537 (1985). *See also* United States v. Twelve 200-Ft. Reels of Super 8MM. Film, 413 U.S. 123, 125 (1973) ("Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry."). 19 U.S.C. § 1581(a) provides that customs officials "at any time [may] go on board of any vessel or vehicle . . . and examine, inspect, and search the vessel or vehicle and every part thereof . . . ." That statute is derived from a statute passed by the First Congress, *see Villamonte*-Marquez, 462 U.S. at 584 (citing the Act of Aug. 4, 1790, ch. 35, § 31, 1 Stat. 164) which "authorized customs officers to board and search vessels bound to the United States and to inspect their manifests, examine their cargoes, and prevent any unlading while they were coming in." Maul v. United States, 274 U.S. 501, 505 (1927).

The earliest customs statute, Act of July 31, 1789, ch. 5, 1 Stat. 29, was passed two months before Congress proposed the Bill of Rights and contained an "acknowledgment of plenary customs power" to conduct warrantless inspections of vessels. United States v. Ramsey, 431 U.S. 606, 616 (1977). The 1789 Act granted customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed;" in contrast, searches of any "particular dwelling-house, store, building, or other place" were authorized with a warrant upon "cause to suspect." § 24, 1 Stat. 43. That provision was carried forward in the Act of Aug. 4, 1790, ch. 35, § 48, 1 Stat. 170, and is distinct from the separate authority of customs to conduct suspicionless searches of articles and effects when presented for entry at the border. Because the 1790 Act was passed by the same Congress that promulgated the Fourth Amendment, "it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment." *Ramsey*, 431 U.S. at 617 (quoting Boyd v. United States, 116 U.S. 616, 623 (1886)).

[7] Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979).

[8] United States v. Ramsey, 431 U.S. 606, 619 (1977).

> Time and again, we have stated that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[9]

The Supreme Court has never invalidated a search or seizure at the border. Obscuring the clarity of that fact and the underlying border doctrine principles are two aspects of the Court's cases. First, as the balancing test to measure reasonableness became prevalent in the latter part of the twentieth century,[10] that test began to insinuate itself into the border doctrine opinions, even as the Court was noting that "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border. . . ."[11] Second, some of the Court's opinions have stated that, for intrusions beyond the scope of "routine" customs searches and inspections, the individual liberty interest protected by the Fourth Amendment is not outweighed by mere assertions of sovereignty and, in the balance of interests, individualized suspicion of illegal activity becomes necessary.[12] Hence, in *United States v. Montoya de Hernandez*,[13] the Court upheld the sixteen-hour detention of a person reasonably suspected to be a "balloon swallower," which is a method of smuggling narcotics into the country by hiding them in the person's alimentary canal.[14] In contrast to "[r]outine searches of the persons and effects of entrants . . . ," which are not "subject to any requirement of reasonable suspicion, probable cause, or warrant,"[15] the detention in *Montoya de Hernandez* was viewed as nonroutine, but was nevertheless upheld, with the Court applying a balancing test:

---

[9] United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

[10] *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 11.3.4 (Carolina Academic Press 2008).

[11] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985). *See also* United States v. Ramsey, 431 U.S. 606, 616 (1977).

[12] *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

[13] 473 U.S. 531 (1985).

[14] *Id.*

[15] *Id.* at 538.

> We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.[16]

In *Montoya de Hernandez*, the Court noted that it was expressing no view "on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."[17] In contrast, Justice Stevens, in his concurring opinion, believed that customs agents could "require that a nonpregnant person reasonably suspected of this kind of smuggling submit to an x-ray examination as an incident to a border search."[18] Justice Brennan, dissenting, believed that travelers at the border could be routinely "subjected to questioning, patdowns, and thorough searches of their belongings."[19] He believed that "body-cavity searches, x-ray searches, and stomach pumping" were "highly intrusive investigative techniques" that must be authorized by a judicial officer.[20]

Lower courts and commentators have used variations of the balancing test and the distinction between routine and nonroutine intrusions to evaluate border searches and seizures. There are two issues here: the distinction between routine and nonroutine intrusions, and the needed level of suspicion to justify those intrusions. As to the first, a vague and somewhat

---

[16] *Id.* at 541. *Cf.* United States v. Flores-Montano, 541 U.S. 149, 155 n.3 (2004) (observing that delays of "one to two hours at international borders are to be expected.").

[17] 473 U.S. at 541 n.4.

[18] *Id.* at 545 (Stevens, J., concurring).

[19] *Id.* at 551 (Brennan, J., dissenting).

[20] *Id. Cf.* United States v. Lawson, 461 F.3d 697, 700 (6th Cir. 2006) ("As to the x-ray of her luggage, the officers did not need reasonable suspicion before undertaking this examination, one that has become a customary feature of commercial airline travel. An x-ray examination of a *person,* it is true, may require some level of suspicion because it may present risks to health that an x-ray examination of luggage will not present and because it may permit greater intrusions into the privacy and dignity of the individual."). *See generally* Lauren Bercuson, Comment, *Picture Perfect? X-Ray Searches at the United States Border Require Guidance*, 35 U. MIAMI INTER-AM. L. REV. 577 (2004) (discussing courts' treatment of x-rays at the border and medical issues involved).

complex jurisprudence[21] attempting to distinguish between the two types of intrusions had developed prior to *United States v. Flores-Montano,*[22] with the courts creating lists of routine and nonroutine searches.[23] For example, patdowns[24] and shoe checks[25] are generally considered routine, but body cavity[26] or strip searches[27] are not.

As to the level of suspicion needed, several decades of development created some unusual standards of reasonableness. For example, a "real suspicion" was said to justify a strip search,[28] a "clear indication" that a suspect was carrying contraband in a body cavity justified that examination,[29] but only a "minimal showing of suspicion" was needed for a

---

[21] *See, e.g.,* United States v. Molina-Tarazon, 279 F.3d 709, 713 (9th Cir. 2002) (border "searches of handbags, luggage, shoes, pockets and the passenger compartments of cars are clearly routine . . ." and may be conducted without reasonable suspicion and "the distinction between 'routine' and 'nonroutine' turns on the level of intrusiveness [of the search]."); United States v. Robles, 45 F.3d 1, 5 (1st Cir. 1995) (noting that "[t]he government concedes that drilling a hole in the cylinder was nonroutine," and having "little difficulty concluding that drilling a hole into the cylinder was not a routine search"); United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988) (outlining the following factors for consideration in analyzing the invasiveness of a border search: "(1) whether search results in exposure of intimate body parts or requires suspect to disrobe; (2) whether physical contact between Customs officials and the suspect occurs during the search; (3) whether force is used to effect the search; (4) whether the type of search exposes the suspect to pain or danger; (5) the overall manner in which the search is conducted; and (6) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search.") (internal citations omitted).

[22] 541 U.S. 149 (2004).

[23] *E.g.,* Tabbaa v. Chertoff, 509 F.3d 89, 98 (2d Cir. 2007); United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006).

[24] *E.g.,* Kaniff v. United States, 351 F.3d 780, 784-88 (7th Cir. 2003) (collecting cases); Davis v. State, 754 A.2d 1111, 1114 (Md. Ct. Spec. App. 2000). *Cf.* United States v. Vance, 62 F.3d 1152, 1156 (9th Cir. 1995) (requiring "minimal" suspicion for patdown).

[25] *E.g.,* United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994).

[26] *E.g.,* United States v. Des Jardins, 747 F.2d 499, 505 (9th Cir. 1984).

[27] *E.g.,* United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); United States v. Oyekan, 786 F.2d 832, 837 (8th Cir. 1986); State v. Green, 787 A.2d 186, 195 n.9 (N.J. Super. Ct. App. Div. 2001). *Cf.* United States v. Braks, 842 F.2d 509, 513 (1st Cir. 1988) (lifting up of skirt by defendant in private room revealing bulge of drugs in girdle considered routine border search); Davis v. State, 754 A.2d 1111, 1114 (Md. Ct. Spec. App. 2000) ("Only strip searches and body cavity searches consistently have been considered non-routine.").

[28] United States v. Guadalupe-Garza, 421 F.2d 876, 879 (9th Cir. 1970).

[29] United States v. Des Jardins, 747 F.2d 499, 505 (9th Cir. 1984).

patdown.[30] These standards developed in the wake of *Terry v. Ohio*,[31] where it appeared that the individualized suspicion standard would become multiplicitous. That did not happen[32] and, indeed, in the context of a border seizure, the Court explicitly stated in *United States v. Montoya de Hernandez*[33] that it was rejecting reasonableness standards of individualized suspicion beyond reasonable suspicion and probable cause. Nonetheless, lower courts continue to use language suggesting different measures of reasonableness, albeit some have attempted to retrofit their jurisprudence to be consistent with Supreme Court case law.[34] Currently, the prevailing view appears to be that, for intrusive searches and seizures at the border, reasonable suspicion is needed.[35]

So how viable is the distinction between routine and nonroutine intrusions? In *United States v. Flores-Montano*,[36] the Court addressed the question whether customs officers at the international border must have reasonable suspicion to remove, disassemble, and search a vehicle's fuel tank for contraband.[37] The district court had granted suppression on the basis of Ninth Circuit precedent requiring reasonable suspicion for "nonroutine" border searches, and the appellate court had summarily affirmed.[38] Flores-Montano arrived at a border crossing in a station wagon and, although the facts suggested

---

[30] United States v. Des Jardins, 747 F.2d 499, 505 (9th Cir. 1984); United States v. Vance, 62 F.3d 1152, 1156 (9th Cir. 1995).

[31] 392 U.S. 1 (1968).

[32] *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 6.3.2. (Carolina Academic Press 2008).

[33] 473 U.S. 531, 541 (1985).

[34] *E.g.*, United States v. Oyekan, 786 F.2d 832, 837 (8th Cir. 1986) (equating "real suspicion" with articulable suspicion, which justifies a strip search); State v. Green, 787 A.2d 186, 195 n.9 (N.J. Super. Ct. App. Div. 2001) (same and asserting need for articulable suspicion for nonroutine searches such as strip searches).

[35] *E.g.*, United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); Kaniff v. United States, 351 F.3d 780, 784-88 (7th Cir. 2003); United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994); United States v. Oyekan, 786 F.2d 832, 837 (8th Cir. 1986); State v. Green, 787 A.2d 186, 195 n.9 (N.J. Super. Ct. App. Div. 2001).

[36] 541 U.S. 149 (2004).

[37] *Id.* at 152.

[38] *Id.* at 151.

that there was reasonable suspicion of criminal activity,[39] the federal government declined to argue the point because it wanted to test the Ninth Circuit precedent.[40] A customs inspector, after brief questioning and tapping of the gas tank of the vehicle, referred Flores-Montano to a secondary station.[41] After more tapping, a mechanic was called, who arrived twenty to thirty minutes later.[42] The car was raised on a lift, the gas tank removed and disassembled, and marijuana recovered from inside of it.[43] "Th[at] process took [about] 15 to 25 minutes."[44]

The Supreme Court unanimously found that the search was reasonable, with the Court maintaining that customs authorities have plenary authority to conduct such a search.[45] The Court grounded its view on the belief that border searches are intrinsic to sovereignty, that there was significant historical support for such searches, that Congress had consistently authorized border intrusions, and that the government had a "paramount interest in protecting the border."[46] Addressing the viability of the distinction between "routine" and "nonroutine border searches," the Court asserted:

> [T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person–dignity and privacy interests of the person being searched–simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles.
>
> The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, we have stated that

---

[39] *See, e.g., id.* at 150-51.
[40] *See id.* at 151.
[41] *Id.* at 150-51.
[42] *Id.* at 151.
[43] *Id.*
[44] *Id.*
[45] *Id.* at 155.
[46] *Id.* at 152-53.

> "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[47]

Keeping open the possibility that some intrusions may be unreasonable, *Flores-Montano* specifically referenced drilling into vehicles and, quoting *Ramsey*,[48] expressed no view on "'whether, and under what circumstances, a border search might be deemed unreasonable because of the particularly offensive manner it is carried out.'"[49] The Court did not, however, repeat the routine-nonroutine distinction of previous cases.[50]

In light of *Flores-Montano*, some lower court opinions are setting aside the routine-nonroutine distinction, as applied to searches of objects, and instead are focusing on the manner in which the search was conducted.[51] Hence, in *United States v. Hernandez*,[52] the Ninth Circuit observed that the "routine/non-routine analytical framework has been denounced by the Supreme Court insofar as searches of property are concerned."[53] The *Hernandez* court applied *Flores-Montano* to

---

[47] *Id.* at 152-53 (citation omitted).

[48] United States v. Ramsey, 431 U.S. 606, 616 (1977).

[49] 541 U.S. at 155 n.2. *Cf.* United States v. Lawson, 461 F.3d 697, 702 (6th Cir. 2006) ("customs officers . . . did not violate . . . Fourth Amendment when they cut the liner [of traveler's] luggage, then drilled a hole in it"); United States v. Hernandez, 424 F.3d 1056, 1057 (9th Cir. 2005) ("initial search of the vehicle, which involved merely pulling back the interior panels of the doors on the vehicle in such a manner that they could be replaced without damage, was not especially destructive or otherwise carried out in an offensive manner"); United States v. Chaudhry, 424 F.3d 1051, 1053 (9th Cir. 2005) (concluding "that a single 5/16-inch hole drilled in the bed of a pickup truck does not require reasonable suspicion . . . .").

[50] *Id.*

[51] *See* United States v. Romm, 455 F.3d 990, 997 n.11 (9th Cir. 2006) (interpreting *Flores-Montano* to suggest "that the search of a traveler's property at the border will always be 'routine' . . . ."). Other courts continue to use the routine–non-routine framework. *E.g.*, United States v. Whitted, 541 F.3d 480, 485-86 (3d Cir. 2008) (maintaining routine–non-routine framework and holding that search of passenger cabin of cruise ship returning to the United States required reasonable suspicion).

[52] 424 F.3d 1056 (9th Cir. 2005).

[53] *Id.* at 1058 n.2. *See also* United States v. Cortez-Rocha, 394 F.3d 1115, 1119-20 (9th Cir. 2005) (holding that destruction of spare tire not unreasonably destructive and

the situation in which customs officials removed a door panel on a vehicle:

> [T]he initial search–which involved removal of the interior door panels in "an easy way, [so] that if we [don't] find anything [we] can put it back together without damage. Very gently"–caused no significant damage to, or destruction of, the vehicle. Nor did it undermine the safety of the vehicle, or present any potentially harmful effects to the health of the motorist. . . . [T]he damage involved through the removal of the door panel in this case was minimal. In short, the gentle removal of the door panel was not "so destructive as to require a different result." . . . Neither can it be said that the search was conducted in a particularly offensive manner. . . . Therefore, reasonable suspicion was not required prior to conducting the search.[54]

LETTERS AND DATA AS TARGETS; THE TECHNOLOGICAL BORDER

In *United States v. Ramsey*,[55] the Court was confronted with a situation in which a customs official, based on reasonable suspicion, opened letters mailed from Bangkok, Thailand, to addresses in Washington, D.C.[56] Congress and applicable postal regulations had authorized the opening of an envelope if there

---

observing that, "[a]lthough cutting a spare tire is certainly damaging to that tire, the important factor is whether the procedure results in significant damage to, or destruction of, the vehicle," with a focus on "operation of the vehicle . . . ."); United States v. Camacho, 368 F.3d 1182, 1186 (9th Cir. 2004) (upholding suspicionless border search in which officers used radioactive density meter called "Buster" to search inside of spare tire); United States v. Bennett, 363 F.3d 947, 951 (9th Cir. 2004) (noting that, although most border searches involving vehicles do not require any articulable level of suspicion, "especially destructive searches of property . . . may require reasonable suspicion."). *But cf.* Recent Case, *United States v. Cortez-Rocha, 394 F.3d 1115 (9th Cir. 2005)*, 118 HARV. L. REV. 2921 (2005) (criticizing court's methodology and stating that "the Ninth Circuit should have seized the opportunity to impose a balancing test for determining the reasonableness of destructive border searches, thereby according principled protection to Fourth Amendment rights in a context where such protection is sorely needed.").

[54] *Hernandez*, 424 F.3d at 1059. The court added that, "[o]nce the initial package of marijuana was found, of course, the officers had ample suspicion to justify the further removal of, and damage to, the door panels, glove box and other components of the vehicle, in an effort to locate additional stashes of marijuana." *Id.* at 1059 n.5.

[55] 431 U.S. 606 (1977).

[56] *Id.* at 608.

was "reasonable cause to suspect" that there was merchandise imported contrary to the law.[57] The Court upheld the inspection, which uncovered heroin in each of the envelopes.[58] Addressing the "fear that '[i]f the Government is allowed to exercise the power it claims, the door will be open to the wholesale, secret examination of all incoming international letter mail,'"[59] the Court concluded that that concern was not present in the case before it:

> Here envelopes are opened at the border only when the customs officers have reason to believe they contain other than correspondence, while the reading of any correspondence inside the envelopes is forbidden. Any "chill" that might exist under these circumstances may fairly be considered not only "minimal," but also wholly subjective.[60]

Although reasonable suspicion was present, and the Court found the search justified on that ground, much of the opinion takes a much broader view of governmental authority at the border. The Court rejected the view that letter envelopes should be treated differently than other packages or wrappers:

> It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical. It was conceded at oral argument that customs officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Surely no different constitutional standard should apply simply because the envelopes were mailed not carried. The critical fact is that the envelopes cross the border and enter this country, not that that [sic] are brought in by one mode of transportation rather than another. It is their entry into this country from without it that makes a resulting search "reasonable."[61]

The *Ramsey* Court continued:

---

[57] *Id.* at 611.

[58] *Id.* at 612.

[59] *Id.* at 632.

[60] *Id.* at 624 (internal citations omitted).

[61] *Id.* at 620 (internal citations omitted).

> Almost a century ago this Court rejected such a distinction in construing a protocol to the Treaty of Berne, 19 Stat. 604, which prohibited the importation of letters which might contain dutiable items. *Cotzhausen v. Nazro*, 107 U.S. 215 (1883). Condemning the unsoundness of any distinction between entry by mail and entry by other means, Mr. Justice Miller, on behalf of a unanimous Court, wrote:
>
> "Of what avail would it be that every passenger, citizen and foreigner, without distinction of country or sex, is compelled to sign a declaration before landing, either that his trunks and satchels in hand contain nothing liable to duty, or if they do, to state what it is, and even the person may be subjected to a rigid examination, if the mail is to be left unwatched, and all its sealed contents, even after delivery to the person to whom addressed, are to be exempt from seizure, though laces, jewels, and other dutiable matter of great value may thus be introduced from foreign countries."
>
> The historically recognized scope of the border-search doctrine, suggests no distinction in constitutional doctrine stemming from the mode of transportation across our borders.[62]

Accordingly, *Ramsey* rejected the dissent's view that Congress had shown heightened respect for "the individual's interest in private communication,"[63] finding that "no such support may be garnered from the history of the Fourth Amendment insofar as border searches are concerned."[64] The majority also rejected any distinction "between letters mailed into the country, and letters carried on the traveler's person."[65]

There are several significant intimations in *Ramsey*, given

---

[62] *Id.* at 620-21.

[63] *Id.* at 626 (Stevens, J., dissenting).

[64] *Id.* at 612 n.8 (majority opinion).

[65] *Id.* at 623; *see also id.* at 623 n.16. *See also* United States v. Fortna, 796 F.2d 724, 738-39 (5th Cir. 1986) (upholding suspicionless document search at border); United States v. Soto-Teran, 44 F. Supp. 2d 185, 190-91 (E.D.N.Y. 1996) (upholding suspicionless inspection of sealed envelope and cursory inspection of letter but indicating that close reading needed reasonable suspicion), *aff'd*, 159 F.3d 1349 (2d Cir. 1998).

the migration of so much information to digital form and the ability to send it anywhere in the world where there is an Internet connection. First, what about searches that examine digital data on computers and other storage devices at the border? Given that computers and other electronic devices can hold legally excludable information, do federal agents have the right to examine devices that could store such information? *Ramsey* clearly permits reasonable suspicion based searches if it is accepted that data on a computer are the functional equivalent of a writing and that a computer file is the electronic equivalent of an envelope.[66] But are suspicionless searches permitted? Here, one may seek to distinguish between mail, which is regulated by statutory and postal regulations, and digital data, which is not. *Ramsey*, however, rejected such a distinction.[67] Nonetheless, First Amendment and privacy concerns seem to lurk.

In *United States v. Arnold*,[68] the district court asserted that reasonable suspicion was required to conduct searches of laptop computers at the border. The court concluded:

> Fourth Amendment protection extends to the search of this type of personal and private information at the border. While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound. Therefore, government intrusions into the mind–specifically those that would cause fear or apprehension in a reasonable person–are no less deserving of Fourth Amendment scrutiny than

---

[66] *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 12.4.8. (Carolina Academic Press 2008).

[67] *Ramsey*, 431 U.S. at 623-24. *Cf.* California Bankers Ass'n v. Shultz, 416 U.S. 21, 62-63 (1974) (upholding regulations requiring banks to report commercial transactions that "take place across national boundaries" against a Fourth Amendment challenge based in part on the border doctrine).

[68] 454 F. Supp. 2d 999 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008).

intrusions that are physical in nature.[69]

Arnold is difficult to reconcile with the broad searches approved of at the border by Supreme Court cases, which make no distinction based on the objects sought (so long as it is not a search of a person) and the methods employed (so long as they are not particularly destructive). Other courts, including the Ninth Circuit which reversed the lower court's decision in *Arnold*, examining the question of whether customs agents can search the files on a computer at the border have rejected the reasoning underlying the district court's opinion in *Arnold*.[70] Thus, in *United States v. Ickes*,[71] the court viewed computer files the same as any other "cargo" subject to inspection at the border. The court noted:

> Particularly in today's world, national security interests may require uncovering terrorist communications, which are inherently "expressive." Following Ickes's logic would create sanctuary at the border for all expressive material–even for terrorist plans. This would undermine the compelling reasons that lie at the very heart of the border search doctrine.[72]

Ickes added that a distinction grounded on First Amendment materials would be impractical and unwarranted, based on case law rejecting heightened protections from searches and seizures for First Amendment materials.[73] The *Ickes* court also observed that, as a practical matter, computer

---

[69] Arnold, 454 F. Supp. 2d at 1000-01. *See also* Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971 (2007) (asserting that laptop searches at the border must be justified by articulable suspicion).

[70] *See* United States v. Romm, 455 F.3d 990, 997, 997 n.11 (9th Cir. 2006) (positing laptop search was routine border search and interpreting *Flores-Montano* to suggest "that the search of a traveler's property at the border will always be deemed 'routine'," including search of computers); People v. Endacott, 79 Cal. Rptr. 3d 907, 909 (Cal. Ct. App. 2008) (upholding suspicionless border search of laptop computers). *Cf.* United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (declining to decide whether examination of computer disks routine or nonroutine search because search supported by reasonable suspicion); United States v. Roberts, 274 F.3d 1007 (5th Cir. 2001).

[71] 393 F.3d 501 (4th Cir. 2005).

[72] *Id.* at 506.

[73] *Id.* at 506-07.

searches at the border were not likely to occur unless the traveler's conduct or other facts suggested a need for further search.[74] The court maintained: "The essence of border search doctrine is reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements applied to the inapposite context of this sort of search."[75] Such discretionary limitations on border searches are, one could argue, none at all—but that is, it appears, the essence of the border search doctrine.[76]

Putting aside the question of how intrusive a search or seizure can be, perhaps a more difficult question presented by today's world is how to define the border.[77] The Court's cases all

---

[74] *Id.* at 507.

[75] *Id.*

[76] *See* Kelly A. Gilmore, Note, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border,* 72 BROOK. L. REV. 759 (2007) (arguing that border search doctrine applies to permit suspicionless searches of laptop computers and electronic hand-held devices such as PDAs and iPods).

[77] *Compare* David R. Johnson & David Post, *Law and Borders–the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1400 (1996) (arguing that new rules must govern the Internet that should be distinct from the "current territorially based legal systems") *with* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1201 (1998) (arguing "that regulation of cyberspace is feasible and legitimate from the perspective of jurisdiction and choice of law."). Goldsmith cites examples of nation-states regulating content on the Internet within their borders:

> A government can choose to have no Internet links whatsoever and to regulate telephone and other communication lines to access providers in other countries. China, Singapore, and the United Arab Emirates have taken the somewhat less severe steps of (i) regulating access to the Net through centralized filtered servers, and (ii) requiring filters for in-state Internet service providers and end-users . . . . Germany has chosen to hold liable Internet access providers who have knowledge of illegal content and fail to use "technically possible and reasonable" means to filter it.

Id. at 1227-28. He also notes:

> Cyberspace information can only appear in a geographical jurisdiction by virtue of hardware and software physically present in the jurisdiction. Available technology already permits governments and private entities to regulate the design and function of hardware and software to facilitate discrimination of cyberspace information flows along a variety of dimensions, including geography, network, and content.

Id. at 1225-26. Whether it is permissible under the United States Constitution to restrict access to the Internet is not the question here; it is whether the sovereign power permits the government to search and seize data that violates the laws of the United States or is otherwise excludable. Goldsmith's article indicates that foreign governments recognize that the international border may be digital in nature. *See also* Harvey

concern the physical border or its functional—but still physical—equivalent. Hence, a person at the border with a laptop is still at the border. Instead, what if that person, while in a foreign country, emailed child pornography images to his home computer, which is located in the United States? If a letter can be searched coming into the country, what about emails, their attachments, or other forms of electronic communications? If they cannot, what is to stop the wholesale creation of offshore businesses specializing in child pornography, illegal gambling, or copyright violations? What is to stop the digital transfer of terrorist plans?[78] On the other hand, in today's world, the most routine in-state phone call may be routed to a satellite; an email to someone in the United States from someone in the United States may pass anywhere over the Internet. Are such communications now permissibly examined as border searches? One possible solution to such a quandary is to find the border search doctrine inapplicable, based on the wholly intra-national nature of the origin and destination of the

---

Rishikof, *Long Wars of Political Order–Sovereignty and Choice: the Fourth Amendment and the Modern Trilemma,* 15 CORNELL J.L. & PUB. POL'Y 587, 618 (2006) (concluding that "[a] political order with international penetrating and expansive technology for counterintelligence purposes will come at the expense of privacy, personal autonomy, and sovereignty as borders and transportation become increasingly transparent. This new political order will be very different from the classic 19th century liberal state, which for the last 200 years has been the ideal model of personal autonomy.").

[78] In response to criticisms of its intelligence interception program implemented in response to the 2001 terrorists attacks on the United States, the Bush Administration released a paper entitled: "Legal Authorities Supporting Activities of the National Security Agency Described by the President" (U.S. Department of Justice 01/19/06). That paper discussed the "intercept[ion] of international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations." *Id.* at 1. The report grounded the authority to do so on the president's inherent powers in national security matters and in Congressional authorizations after 9/11. *See id.* Remarkably, it did not ground that authority on the border search doctrine. Indeed, it merely noted that the activities were consistent with the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and added that "the monitoring of international communications into or out of the United States of U.S. citizens" was not regulated by FISA. *Id.* at 19 n.6. In the section addressing Fourth Amendment concerns, the paper asserted that the actions are justified by reference to the balancing test to measure reasonableness and observed that the only targets of the international communications intercepts were those who were reasonably suspected to be agents of al Qaeda or an affiliated organization. *See id.* at 41.

communication, ignoring the technical means by which the communication is achieved. This functional approach satisfies the sovereignty concerns underlying the border search doctrine.

ARTICLES FOR THIS SYMPOSIUM

The contributors to this symposium offer a variety of views on these difficult issues. Professor Palfrey in his article, *The Public and the Private at the United States Border with Cyberspace*, provides background on the "points of control" where data may be obtained and the methods by which governments and private parties collect digital information about citizens and others.[79] As he observes: "In the twenty-first century, a state can come to know more about each of its citizens via surveillance than ever before in human history."[80] Although he recognizes that the Fourth Amendment has been held not to apply to data collected by a private third party, he maintains that "[t]he meaning of the public and the private is changing, in material ways, both from the perspective of the observer and the observed. We need to rethink legal protections for citizens from state surveillance in a digital age as a result of this third-party data problem."[81] He argues for a "sliding scale . . . to distinguish between those transactions . . . that use digital networked technologies that give rise to some legal protection and those that do not."[82]

Professor Robert M. Bloom, in his article, *Border Searches in the Age of Terrorism*, offers a caution in the concluding sentence of his contribution to this symposium: "If the war on terrorism is fought in a way that ignores our democratic ideals, we have lost the war."[83] Prior to that caution, he examines the history of the border search doctrine, including an examination of the significant reorganization of the border enforcement

---

[79] John Palfrey, The Public and the Private at the United States Border with Cyberspace, 78 MISS. L.J. 241 (2008).

[80] *Id.*

[81] *Id.* at 242.

[82] *Id.* at 289.

[83] Robert Bloom, Border Searches in the Age of Terrorism, 78 MISS. L.J. 295, 327 (2008).

apparatus resulting from 9/11.[84] In his view, the border search doctrine fits comfortably within the Supreme Court's balancing test to measure reasonableness, and the routine–non-routine distinction remains a viable analytical structure. He observes: "Routine versus non-routine distinction usually focuses on the physical aspects of the search, such as disrobing, exposing intimate body parts, forced intrusions causing pain, and physical contact."[85] Hence, "[w]hen the scope of the intrusion increases to the extent that the border search is no longer routine, then some justification might be required."[86] Professor Bloom applies that framework to a variety of circumstances, including computer searches, which he believes should require "some level of justification."[87] His final focus is on Fourth Amendment cases involving terrorism concerns after 9/11, and he uses them to draw "some conclusions about the effect the emerging emphasis on terrorism and national security concerns will likely have on border searches in this post-9/11 world."[88]

Professor Susan Freiwald, in *Electronic Surveillance at the Virtual Border*, offers a summary of the treatment of the interception of two forms of electronic communication: traditional telephone calls, and email.[89] Her purpose is to consider "how the law has created intangible borders to regulate government surveillance of communications" and that those "intangible borders function the same way as traditional physical borders functioned historically" in that they "demarcate those 'places' in which our government imposes burdens and grants privileges from those 'foreign places' in which it does neither."[90] Freiwald observes that the legal framework for intercepting telephone calls creates a virtual border, depending largely upon who the target of the investigation is. Thus,

---

[84] *Id.* at 300-17.

[85] *Id.* at 310 n.92.

[86] *Id.* at 305.

[87] *Id.* at 315.

[88] *Id.* at 300.

[89] Susan Freiwald, *Electronic Surveillance at the Virtual Border*, 78 MISS. L.J. 329 (2008).

[90] *Id.* at 331.

electronic surveillance law has determined "when foreign persons acquire Fourth Amendment protections and when U.S. Persons lose them."[91]

Professor Matthew R. Hall, in his essay entitled *Border Fiction: Does an Analogy to Immigration Law Alleviate Fourth Amendment Anxiety?*, offers some analogies to immigration law's treatment of the border.[92] His essay applies elements of that analogy to electronic communications and to physical entries into the country. He also offers some reflections on assumptions that immigration law uses about the mental state of individuals who cross the border and suggests that the "federal government might consider the delegation of border doctrine responsibilities to state and local officials."[93] He ultimately concludes that the most important contribution an immigration law analogy would have is the use of a "cost-benefit analysis" for border searches similar to what "courts do when considering the constitutionality of immigration procedures under the constitutional guarantee of procedural due process."[94]

The final contributor, Professor Harvey Rishikof, in *Combating Terrorism in the Digital Age: A Clash of Doctrines*, examines the challenges confronting the nation as the three branches of government seek to address the issues described in the title to his article.[95] He offers observations on the relationship of critical trends in the marketplace, the nature of modern threats to the state, theories of sovereignty, and Supreme Court analysis of the Fourth Amendment. He articulates a series of propositions: the "digital information super highway is *omnipresent* and *omniaccessible* and *irreversible*;"[96] the "threats are individualized, multivaried, potentially lethal on a mass scale, and potentially devastatingly

---

[91] *Id.* at 361.

[92] Matthew R. Hall, *Border Fiction: Does an Analogy to Immigration Law Alleviate Fourth Amendment Anxiety?*, 78 MISS. L.J. 363 (2008).

[93] *Id.* at 364.

[94] *Id.* at 380.

[95] Harvey Rishikof, *Combating Terrorism in the Digital Age: A Clash of Doctrines: The Frontier Of Sovereignty—National Security And Citizenship—The Fourth Amendment—Technology And Shifting Legal Borders*, 78 MISS. L.J. 381 (2008).

[96] *Id.* at 385.

costly;"[97] there is a "clear and justified need" to patrol the border;[98] and all nations view borders as "unique areas of sovereign power that trump both domestic and international norms."[99] Professor Rishikof believes that these propositions create "a social force of extreme state anxiety over border control."[100]

Turning specifically to combating terrorism in the digital age, he maintains that, to be successful, "a 'sea' of information" must be analyzed.[101] Yet, he asserts, the executive, legislature, and courts have approached the propositions he sketches from their own "institutional competencies," resulting in "unsatisfactory from all policy perspectives."[102] He offers several prescriptions for reform, including institutional reform of the intelligence and law enforcement communities, ending the "debate over executive authority and congressional reticence," including the judiciary in surveillance activities, and adopting a more international approach to the issues.[103] Professor Rishikof concludes that this is "a challenge we must meet" because "so much is at stake" and "how we treat borders and data will define the power of the state and privacy in the twenty-first century."[104]

---

[97] *Id.* at 390.
[98] *Id.*
[99] *Id.* at 393.
[100] *Id.*
[101] *Id.* at 400.
[102] *Id.* at 428.
[103] *Id.* at 429.
[104] *Id.* at 430.

THE PUBLIC AND THE PRIVATE AT THE UNITED STATES BORDER WITH CYBERSPACE

*John Palfrey**

ABSTRACT

In the twenty-first century, a state can come to know more about each of its citizens via surveillance than ever before in human history. Some states are beginning to exercise this ability. Much of this additional surveillance ability derives from enhanced access to digital information. This digital information comes in the form of bits of data that flow through both rivers and oceans of data. These rivers are full of information that passes by a given point, or series of points, in a network and can be intercepted; these oceans are also stocked with information that can be searched after the fact. These data are held in

---

* Henry N. Ess III Professor of Law and Vice Dean of Library and Information Resources at Harvard Law School and a faculty director of the Berkman Center for Internet & Society at Harvard University. This paper was commissioned and underwritten by funds from the National Center for Justice and the Rule of Law at the University of Mississippi School of Law (National Center), which is supported by a grant from the Office of Justice Programs at the United States Department of Justice. The research on Internet surveillance included in this paper was also supported by a grant from the John D. and Catherine T. MacArthur Foundation. The author gratefully thanks Hal Roberts for his research on the three levels of surveillance, development of draft sections of this paper, and shrewd editorial suggestions. Terry Fisher, Christopher Soghoian, Dr. Robert Faris, and Chris Conley offered important technical and editorial assistance. In addition, Virginia Farmer deserves thanks for excellent legal research assistance. Errors and omissions are the author's alone.

private hands as well as public. The most effective (or invasive, depending upon your vantage point) new forms of surveillance often involve a search of data held in a combination of private and public hands. Both private and public entities are increasingly encouraged to retain more data as a result of legal and market pressures. There are essentially no Fourth Amendment protections for U.S. citizens whose data is collected by a private third-party and turned over to the state. Nor are there such constitutional protections for the re-use of privately collected data by state actors. The few statutory provisions that protect citizens in these contexts are out-of-date and riddled with loop-holes. This inquiry prompts hard questions about the need to redefine the public and the private in a digital age. The meaning of the public and the private is changing, in material ways, both from the perspective of the observer and the observed. We need to rethink legal protections for citizens from state surveillance in a digital age as a result of this third-party data problem.

I. INTRODUCTION

> Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive. Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case.[1]

So punted a court in a case related to the privacy implications of police use of a Global Positioning Satellite (GPS) program. This punting was with good reason in this particular case: the court did not need to reach this larger issue to resolve the matter before them. Instead, the court simply wished to draw attention to the bigger problem on the horizon. At some point, each state that cares about the privacy interests of its

[1] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

citizens will have to grapple with this hard question. In the process, we will find that our received notions of what is public and what is private have changed in a digital age in ways that have profound implications for the future.[2]

As a nation that continues to lead in the development of new technologies, we in the United States push information technology harder and further ahead with every passing year. Much of this innovation takes place in the private sector. It is this innovation, in large measure, that makes surveillance of citizens far cheaper, just as the court said in *United States v. Garcia*.[3] The benefits for economic growth and productivity are obvious; we accept this progress as a social good. The long-term costs of this progress, in areas such as privacy, are less obvious.

As consumers and as citizens, we repeatedly trade convenience for control, handing over growing amounts of information about ourselves to others in the process. Our lives are increasingly mediated by digital technologies and described by data held in digital formats. We are racing ahead quickly with the development of new technologies while the institutions—legal and otherwise—designed to protect user privacy have lagged behind. The tradeoffs involved are rarely conscious ones.

This growing problem has its roots in the fact that, as information technologies improve in efficiency and become more integrated in everyday life, fewer and fewer citizens are likely to know what information is being collected about them and by whom. Much of this data collection is conducted not by state actors, but by private parties. Citizens have even less of a sense of how these data are being used, or might be used and re-used in the future. This issue is particularly acute in the context of

---

[2] The United States is not alone in this respect. "Privacy is a protean concept," according to a Canadian Supreme Court opinion, R.V. Tessling, [2004] 3 S.C.R. 432, 434 (Can.). In his opinion, Justice Binnie implies that the decision-makers are avoiding hard questions. The *Tessling* case parallels the landmark United States case, *Kyllo v. United States*, 533 U.S. 27 (2001), in important respects, though the outcomes of the two matters diverge from one another.

[3] *Garcia*, 474 F.3d at 998 ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.").

young people we have surveyed, who are leaving vast tracks behind them as they lead lives substantially mediated by digital technologies.[4]

This lack of information is not just a matter of simple consumer ignorance or lack of attention on the part of citizens. Rather, the primary cause is that the technologies of surveillance in use at any moment, in this digital age, are unknowable even by experts. We have no way of detecting many kinds of prevalent surveillance; those that we can detect are often hopelessly, unknowably complex. Expert computer users are often fooled by whether the antivirus software they are running on their computer is capturing private information about them or not.[5] Virtually no one knows what information is being kept by our Internet Service Provider or e-mail host or search engine, much less what the National Security Agency (NSA) is collecting through the computers it has installed on AT&T's network.[6] And for many working Americans, there is no realistic choice but to rely upon at least some private parties—whether Google, Microsoft or Yahoo! for search, or AT&T, Verizon, or Comcast for data, and so forth—for digital communications services.

The most important aspect of this story of surveillance—and how little citizens know about it—is the change in the interaction between the public and the private. A growing number of private firms are collecting a growing amount of data about individuals. In effect, each individual has a growing "digital dossier," in the words of Professor Daniel Solove, of information held about them in a distributed set of places.[7] The

---

[4] *See* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 17-82 (2008).

[5] The author has seen this dynamic repeatedly in the context of a related research project, StopBadware.org, which provides forums for novices and experts to work together to understand how certain forms of online surveillance work. *See* http://www.stopbadware.org/.

[6] *See* Ryan Singel, *Whistle-blower Outs NSA Spy Room*, WIRED, Apr. 7, 2006, *available at* http://www.wired.com/science/discoveries/news/2006/04/70619 (last visited Sept. 30, 2008).

[7] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2-7 (2004).

rules for how and when the government can access and aggregate these data are few and unclear. Likewise, there are no protections for the re-use of these data among law enforcement authorities once the information is collected, regardless, in fact, of the legality of the original mode of accessing the data. The Fourth Amendment, as currently understood, reaches neither.[8] While some statutes provide limited protection to citizens, these protections are spotty and cover only specific types of information.[9] This fast-growing "third-party data problem" and its implications are the central concerns of this paper.[10]

This paper builds upon our collective understanding of this emerging third-party data problem in the context of current surveillance and data retention practices. The purpose of reviewing these practices in detail is to highlight some of their largest implications for the privacy of individuals. I begin by describing the changes that advances in digital technologies are bringing about for the practice of state surveillance of citizens with the intention of setting those changes into the context of the conception of the public and the private. The trend I underscore here is the greater interaction between the public sector (those in government who wish to learn more about certain citizens) and private actors who either collect information about citizens or who develop the technology to enable monitoring of citizen activity. As a "surveillance-ready" network, the Internet permits surveillance of citizens in more ways than ever before in human history. This surveillance can take place at the network, server, and client levels of the Internet's architecture. At the same time, citizens are unlikely

---

[8] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 444 (1976).

[9] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1085-86 (2002).

[10] Others have taken up aspects of this problem, too, from various perspectives. *See* Solove, *supra* note 9; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (Univ. of Chicago Press 2007); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

to be in a position to keep up with the changes in these technologies and the potential surveillance practices that they permit. In the final section of the paper, I argue that the combination of these factors places increased pressure on the complex—some say unstable—legal doctrine of the "reasonable expectation of privacy."

II. THE DIGITAL DIFFERENCE

Digital technologies, including but not limited to the public Internet, make several crucial differences when it comes to surveillance. One is the rate of change in technology development and usage practices—and the corresponding difficulty for individuals to keep up with these changes.[11] A second is the scale on which activities occur and the potential area of impact of one's actions.[12] Together, these differences brought about by the rise of digital technologies place a great deal of pressure on courts' interpretation of crucial legal doctrines, such as the Fourth Amendment of the United States Constitution.

The rate of change in technology developments, and associated usage patterns, is faster in many respects than it has been in the past. The time is shortened between major changes in societies and markets; the speed of getting to market with a new technology service or product for an entrepreneur is often faster; the time that it takes for an idea or expression to reach many people can be much lower; and so forth. Consider that it was *centuries* between the invention of the first moveable type in China and the printing date of Gutenberg's first bibles, and yet further centuries before those bibles reached wide circulation. In contrast, digital technologies have reached over a billion people within a few *decades* of their invention.[13] The ability to

---

[11] *See generally* JAMES GLEICK, FASTER 83-93 (1999).

[12] This assertion may seem self-evident to some readers, but the Internet today reaches most parts of the globe and can be accessed at little or no cost in public places such as libraries and schools around the world. The impact of an action that takes place in one place—say, New York in the United States—may have reverberations in a place distant in physical terms and in time.

[13] *See* Robert Darnton, *The Library in the New Age*, THE NEW YORK REVIEW OF

do more with digital technologies is outstripping our ability to process what the social implications of these changes may be.

The scale on which these activities take place, and on which they have an impact, is likewise greater than it has been in the past. The reach and effect of actions in digital space, such as publication of data to a digital network, are greater and growing. The potential impact of an idea can be greater; one can reach many more people by way of an audience than ever before; the scale of harm can be greater for a bad act; the scale of entrepreneurial innovations can become enormous very quickly; the amount and timing of capital is changing; and so forth.

The broad effect of these two factors—vastly increased speed and scale in the development and reach of information technologies—is to make it hard to apply and make rules in this field. These changes apply special pressure to existing legal doctrines, which begin to seem inadequate to new tasks of protecting individual privacy. The more technology advances, and the more people use the technology to mediate more aspects of their lives, the less adequate existing legal protections for individual privacy appear. The impact of these frequent and material changes should be to prompt frequent review of existing laws. In other cases, the answer may be to establish creative, flexible institutions to address such problems without the traditional legislative involvement, to the extent that new effective laws cannot be enacted to solve the right problems.[14]

Lawmakers and judges face a significant challenge in keeping up with this rate of change in information technologies. The implications of these shifts are many; those implications may be yet greater in a few short years if the rate of change continues. I emphasize here the implications for the way that we think of the public and the private in law broadly, with

---

BOOKS, Vol. 55, No. 10 (June 12, 2008) (for a general discussion of this transition in information technologies and the rate of change).

[14] *See, e.g.*, JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 170-73, 195-99 (2008). Consider the example of StopBadware.org, a neighborhood watch project on the Internet intended to protect consumers from malicious code through a partnership of private entities, which picks up where classic regulation has left off. *Id.* at 170-73.

special application to the workings of the Fourth Amendment of the United States Constitution.[15] There are yet more profound implications when one thinks of the implications at an international legal level, since the interplay between law enforcement agencies and private parties globally makes the puzzle vastly more complex. And in many states, citizens have far less to protect them from state intrusion than the Fourth Amendment in the United States.

In the context of surveillance and data retention, these two broad changes mean that, over time, more people can come to know more about what others are doing or have done. The technology of the Internet and other digital networks is surveillance-ready, which is to say the technologies are designed in such a way that surveillance is simple to perform at multiple points in the network. There are many "points of control," as Professor Jonathan Zittrain has pointed out, at which a state may seek to block or to copy bits of information.[16] These points of control include international gateways, Internet Exchange Points (IXPs), Internet Service Providers (ISPs), public access points (such as cybercafés, schools, or public libraries), corporate workplaces, technology service providers (such as blogging hosts, for instance), and other networks, like mobile and tracking devices such as GPS systems on vehicles or handheld devices.[17]

III. TYPES OF DIGITAL SURVEILLANCE: NETWORK, SERVER, AND

---

[15] In this paper, I do not make a specific claim as to when a warrant should issue, nor do I cover the specifics of criminal procedure, such as Rule 41 of the United States Federal Rules of Criminal Procedure (FRCP). There has been much work done in terms of how these processes should work by other legal scholars. *See, e.g.*, Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85-135 (2005) ("This article urges legislatures and rules committees to update the statutory rules that govern the warrant process in response to the new challenge of digital searches," including specific proposals to update Rule 41 of the United States FRCP); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531-85 (2005); and Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503-51 (2007).

[16] *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

[17] *See, e.g.*, Marjorie A. Shields, Annotation, *Fourth Amendment Protections, and Equivalent State Constitutional Protections, as Applied to the Use of GPS Technology, Transponder, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft*, 5 A.L.R.6th 385 (2005).

CLIENT

When one thinks of network surveillance, the image of a man wearing headphones (and perhaps chomping on cold pizza) in a van on a stakeout outside a crook's apartment building may leap to mind. It is true that one means of listening in on the conversations of a surveillance target is to seek to intercept information flows across the network, as in a river (and perhaps to copy or store it for later retrieval). But in the digital age, this mode of "tapping" a line is only one of a wide range of types of surveillance available to a law enforcement official—and not necessarily the most efficient, given the architecture and the scale of the network. The use of many more types of data, collected by many different types of actors, makes it much easier in some instances, to reconstruct a past act or to anticipate a future—lawful or unlawful—act.

Given the proliferation of the means of surveillance on digital networks, it is extremely hard to provide a full picture, at any moment, of all possible means of surveillance of a target. Such a description is hard both on the micro level (of analyzing individual surveillance activities) and on the macro level (of setting these practices into the context of the larger technical, social, political, and legal issues in which they are nested).

One reason for the difficulty at the micro level is that Internet surveillance is a "read-only" activity. If surveillance is done well at the network or server level, it is impossible to detect through direct technical means. We cannot detect the fact of surveillance, what data is being surveilled, or who is surveilling the data. At the micro level, it is difficult to detect and verify the data, actors, and uses of the data involved in any well-planned digital surveillance activity.[18]

---

[18] Most of the observations in this section of this paper are derived from an ongoing research project on Internet surveillance at the Berkman Center for Internet & Society at Harvard University, of which the author is principal investigator. Key researchers include Christopher Soghoian, Hal Roberts, and Chris Conley. Others have made similar observations; nothing in this section is groundbreaking in terms of computer science research. *See generally*, David Lyon, *Cyberspace, Surveillance, and Social Control: The Hidden Face of the Internet in Asia*, *in* ASIA.COM: ASIA ENCOUNTERS THE INTERNET 67, 67-82 (Kong Chong Ho, Randy Kluver, Kenneth C.C. Yang eds., 2003);

The simplest example of this sort of difficult-to-monitor surveillance is a monitoring box, placed with care in the closet of an Internet service provider.[19] If that monitoring box is physically connected to the rest of the network with only read (not write) wires coming from the network, it is technologically incapable of writing anything back to the network. Surveillance at the client level is always theoretically detectable, but most client-side surveillance tools are designed to avoid detection and can only be thwarted in this regard by sophisticated detection techniques. This problem of detection limits what we can say definitively about a given surveillance activity at any given moment. Since we cannot know the answer with perfect clarity, we have to look at that larger field of Internet surveillance as a whole to think about the potential data subject to surveillance.

On the macro level, placing Internet surveillance into the larger technical, political, social, and legal landscapes leads to further questions. The questions are large because of the stream of new information about Internet surveillance. Within this stream of information, it is important to distinguish what represents a meaningfully new type of surveillance and what represents another example of an existing type. There is a wide and growing array of potential surveillance tools. A complete catalogue of these devices would not only be dreadfully boring to read, it would almost certainly be incomplete at any given moment in time since Internet-related surveillance is meant to be carried out undetected. All of these various tools interact with each other in complex ways; for instance, the routers that

---

SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000); LAWRENCE LESSIG, CODE 2.0, 200-232 (2006); DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

[19] The range of types of surveillance, by the government and private industry, has been described in many scholarly papers before this one. For one overview, *see* Gattiker, U.E., Holsten, H. & Miller, J.,

User Attitudes Toward Possible Governmental and/or Organizational Surveillance, Monitoring

and/or Eavesdropping on the Internet, EICAR 2000 Best Paper Proceedings, 126-157 (2000), *available at* http://eicar.weburb.dk/past_conferences/2000/papers/Monday/Security%20Trust%20and%20E-commerce/other/Gattiker.pdf (last visited Nov. 25, 2008).

control the network are clients themselves and so are open to the same sorts of questions we ask of other clients (and vulnerable to monitoring by a range of client surveillance tools).

This paper includes a concise—in fact, simplified—picture of the technical landscape of Internet surveillance through a series of examples of data collection that might permit a state to come to know more about a surveillance target. These examples help inform (and are informed by) the technical questions of what data are being *actually* and *potentially* monitored on the Internet and whom we are trusting to access (and potentially copy and re-use) those data. This paper is meant to include enough of the major sorts of Internet surveillance to place any given activity or tool within a useful technical context.

Internet surveillance can be broken down into three primary categories: network, server, and client. The Internet is composed of clients and servers, in essence a series of devices which talk to one another through the network. Every bit of data on the Internet is traveling or residing at one or more of these locations at any given time. As such, any given Internet activity must happen at or across one (or more) of these locations. In some cases, the line between client and server is blurry or non-existent, but the class of nodes that act as servers is large enough that it is useful to distinguish them from (other) clients. In this model, anything residing on the client proper is treated as client-side Internet surveillance, including both software tools like workplace keylogging systems and hardware tools like keyboard tapping devices. Any machine that predominantly accepts requests, processes them, and returns responses is treated as a server. For simplicity, everything in between the client and the server is considered here to be the network, including the wires that the data travels and the routers that direct the traffic.

A. Network Surveillance

At the highest level, a state can practice surveillance of Internet traffic that flows across the network.[20] The point of

---

[20] *See, e.g.*, SOLOVE, THE DIGITAL PERSON, *supra* note 18, 165-87.

control used by the state might exist at the international gateway between two states or at some intermediate point in the network. For those states that aspire to manage the network the most extensively, this control might function roughly as a "border control." In most places, though—and especially the United States—it would not be possible to establish a perfect ring around the geographic boundaries of the state. Some states, such as China and Saudi Arabia, have sought to establish such means of network control. The colorful example of the "great firewall of China" helps in a graphic sense to envision what the Chinese have sought to erect, but the image is only partially accurate; it both overstates the effectiveness of the wall at the national border and understates the extensiveness of the surveillance regime in China. The British Government is reported to be considering a dramatic expansion to their network surveillance capabilities, in the form of a £12 billion surveillance center to monitor and store emails, web surfing records, and phone records on the nation's largest telecommunications networks.[21] Other states use intermediate mechanisms, such as Internet Exchange Points (IXPs), to force large amounts of network traffic to flow through a single point which might then be monitored.[22] In other cases, such as the examples that follow, the point of control is on the network, but does not fall precisely at an international border.

1. Network Surveillance in the United States

In the United States, the passage of the Communications Assistance for Law Enforcement Act (CALEA) in 1994 was a

---

[21] David Leppard, *Government will spy on every call and e-mail*, THE SUNDAY TIMES, Oct. 5, 2008, *available at* http://www.timesonline.co.uk/tol/news/uk/article4882600.ece (last visited Oct 8, 2008); Graham Tibbetts, *Internet black boxes to record every email and website visit*, THE TELEGRAPH, Nov. 6, 2008, *available at* http://www.telegraph.co.uk/news/uknews/3384743/Internet-black-boxes-to-record-every-email-and-website-visit.html (last visited Nov. 11, 2008).

[22] *See e.g.*, Alan Levin, *Creating National Internet Exchange Points in Africa*, International Telecommunications Union Presentation, June 29, 2005, *available at* http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/south-africa-05/presentation_levin-ixp-en.pdf (last visited Nov. 11, 2008) (providing a description of IXPs and their general usage).

watershed event in terms of network surveillance.[23] CALEA requires that telecommunications companies build tools into their telephone networks that allow companies to respond quickly to law enforcement requests for wiretaps.[24] CALEA filled an obvious gap: the growing use of a new generation of digital telephone switches did not inherently provide the same support for wiretapping as the older tools did. In 2005, the Federal Communications Commission (FCC) extended its interpretation of the law to require that Internet Service Providers (including universities, schools, libraries, and other such non-commercial ISPs) provide wiretapping access to a range of Internet data.[25] The accessible data includes voice over IP (VoIP) Internet telephone services, such as Vonage and Skype; data about when and for how long Internet broadband subscribers connect to the Internet; and packet header data (the source and destination addresses and the port number) of all VoIP packets.[26] In order to reduce the high cost of implementing this new interpretation of CALEA, the FCC has ruled that ISPs could forward their entire data stream to an independent "Trusted Third Party" to handle the wiretapping implementation.[27] The effect of this ruling can be to expose the entire data stream of an ISP using this option to a third party.[28] The Department of Justice submitted a petition in 2007, yet to be ruled on, to include the packet header data of all Internet data, not just VoIP data, but web, email, instant message, and all other Internet traffic.[29] CALEA does not provide legal

---

[23] *See* 47 U.S.C. §§ 1001-10 (2008).

[24] *Id.*

[25] *See* Federal Communications Commission, ET Docket No. 04-295 (Sept. 23, 2005), published 70 Fed. Reg. 59, 664 (Oct. 13, 2005).

[26] *See* Federal Communications Commission, *FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps*, Aug. 5, 2005, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A1.pdf (last visited Nov. 11, 2008).

[27] *See* Federal Communications Commission, Order FCC 06-56 (2006).

[28] *Id.*

[29] *See* Susan Crawford blog, CALEA roundup: 2005-2007, *available at* http://scrawford.blogware.com/blog/_archives/2007/8/16/3162684.html (Aug. 16, 2007, 13:24 EDT).

justification for anyone to access the provided data; it only mandates that the ISP build the technical capability to respond to such requests, the legality of which is in turn determined by other rules.[30]

Reports suggest that the U.S. National Security Agency (NSA) is engaged in a much more intrusive form of network surveillance by mining the full stream of data passing through major ISP backbones. AT&T engineer Mark Klein, after reading a story in the *New York Times*, reported that he had seen strange activity in a closet in an AT&T backbone building.[31] Klein had also seen documents describing data mining equipment in that closet.[32] Such a box is likely capable of executing highly sophisticated queries on the data passing through the backbone.[33] It is capable, for instance, of searching for any traffic (local or international) matching any of a set of complex profiles and forwarding the full contents of any matching data to the agency.[34] But a so-called "black box" such as the one described by Klein, located in a closet, is the best example of equipment that is impossible to probe technically. We are left with indeterminate, circumstantial evidence about the existence and functionality of the box. Questions about what data it is actually monitoring and who actually has access to the data remain unanswered.

2. The Public and Private on International Networks: Three Cases

Network-level surveillance is enabled directly by law in some instances. In other cases, private forms of surveillance become possible because of the way that citizens seek to work around the state surveillance. Three network surveillance

---

[30] *Id.*

[31] *See* John Markoff & Scott Shane, *Documents Show Link Between AT&T and Agency in Eavesdropping Case*, N.Y. TIMES, Apr. 13, 2006, at A1, *available at* http://www.nytimes.com/2006/04/13/us/nationalspecial3/13nsa.html (last visited Nov. 25, 2008).

[32] *Id.* at A7.

[33] *Id.*

[34] *Id.* at A8.

examples from outside the United States are instructive in this regard.

a. Sweden: FRA and Relakks

On June 18, 2008, Swedish lawmakers passed a bill giving its National Defense Radio Establishment (Försvarets radioanstalt, or FRA) the authority to monitor, without a warrant, all phone calls and Internet traffic crossing its border.[35] The FRA had previously been responsible only for intercepting radio signals, though there are reports that it has been monitoring phone calls and emails prior to the new law going into effect in 2009.[36] The new law will allow the Swedish government to access not just the data about phone calls and Internet traffic (who talked to whom when), but the content of the traffic itself when it crosses the Swedish border.[37] All Swedish ISPs will be required to install FRA monitoring equipment within their networks.[38]

There are means by which Internet users can avoid such network-level surveillance capabilities, but these means of evading the state's surveillance mechanisms may lead to further surveillance by private parties (which, in turn, might give those data to the very state agencies that the user sought to avoid). Relakks is a privacy and filtering circumvention tool that uses virtual private network (VPN) technology to encrypt and route all of its users' traffic through Sweden.[39] The tool gives its users

---

[35] *See* Sara Sundelius, *Sweden adopts controversial law to allow secret tapping of e-mails, phone calls*, Associated Press, INT'L HERALD TRIBUNE, June 18, 2008, *available at* http://www.iht.com/articles/ap/2008/06/18/europe/EU-GEN-Sweden-E-mail-Spying.php (last visited Nov. 25, 2008).

[36] *See* Svt.se, *Ingen förundersökning mot FRA*, July 14, 2008, *available at* http://svt.se/svt/jsp/Crosslink.jsp?d=22620&a=1173950&lid=puff_1173812&lpos=rubrik (last visited Nov. 25, 2008).

[37] *See* PrivacyInternational.org, *PHR2006 - Kingdom of Sweden*, Dec. 18, 2007, *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559487 (last visited Nov. 25, 2008).

[38] *See* DW-World.de, *Swedish Government Clears Hurdles to Pass Surveillance Bill*, June 19, 2008, *available at* http://www.dw-world.de/dw/article/0,2144,3421627,00.html (last visited Nov. 25, 2008).

[39] *See* https://www.relakks.com/ (last visited Nov. 11, 2008).

privacy from snooping conducted by their own ISPs and consequently provides defense against the network level filtering that the OpenNet Initiative has documented in countries around the world.[40] This network level filtering consists of surveilling a subset of the traffic that crosses the relatively few routers that process nearly all Internet traffic. For instance, dozens of countries filter all Internet traffic crossing the digital border by running filtering software on the small number of routers that connect them to the outside world.[41] Relakks is one of many tools that routes around this network level filtering by encrypting and routing requests through a machine in a non-filtering country. By encrypting the request until it arrives at a machine that reroutes the conversation to the requested site, the circumvention tool prevents the filtering router from determining the location or content of the site. This process of rerouting conversations to shift places on the network is known as proxying. When someone in China uses a circumvention tool hosted in Sweden to proxy-request a page from the BBC's web server, instead of talking directly from China to Britain, the connection goes from China to Sweden and then from the U.S. to Britain (and back along the same route). This form of circumvention can also be effective against other sources of filtering (for instance, school or ISP filtering of music sharing traffic) as well to "country shift" the connection to allow the user to access content that is restricted (filtered) to users connecting from Sweden or Europe. But such re-routed traffic now goes through a state where both a private party and a government agency have the authority to listen to the conversation. The net effect: those trying to evade circumvention or surveillance through Relakks may unwittingly be exposing themselves to (potentially more extensive) surveillance by the FRA.

---

[40] *See* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert, John Palfrey, Rafal Rohozinski, & Jonathan Zittrain eds., Cambridge: MIT Press, 2008).

[41] *See id.*

b. United Kingdom: British Telecom and Phorm

A case involving the giant telecommunications firm, British Telecom (BT), illustrates a similar point. In June and July of 2007, several BT Internet customers noticed strange activity during some of their Internet sessions.[42] Some of the users noticed performance problems; others found that some sites were not loading correctly, and all noticed extraneous traffic to the same system, dns.sysip.net, which was owned by a company, 121Media, that various anti-virus tools reported to be associated with rootkit spyware.[43] One user reinstalled his system from scratch after being told by BT customer service that his computer was likely infected by some sort of malware, only to find the same suspicious activity on the freshly installed system.[44] These users came to the conclusion that BT was involved somehow with 121Media, either intentionally or through some sort of intrusion. In response to questions from the users and from reporter Chris Williams of *The Register*, BT's customer service and its press office insisted that they had nothing to do with the suspicious behavior.[45] Phorm refused to comment.[46] By the end of the month, users reported the disappearance of the suspicious traffic, and chatter about the matter died without further notice.[47]

In February, 2008, Phorm (the new name of 121Media) publicly announced a deal with BT, as well as with other major

---

[42] *See* Posting of Frank Rizzo to thinkbroadband.com, *available at* http://bbs.adslguide.org.uk/showflat.php?Cat=&Board=bt&Number=3047764&page=3&view=expanded&sb=7&o=0&fpart=all&vc=1 (July 2, 2007, 10:35:12 EST) (last visited Nov. 25, 2008).

[43] *See* Posting of Filippo Spike Morelli to SpikeLab.org, *available at* http://www.spikelab.org/blog/btProxyHorror.html (July 9, 2007) (last visited Nov. 25, 2008).

[44] *See* Ryan Naraine, *Spyware, Rootkit Maker Stops Distribution*, eWeek.com, May 10, 2006, *available at* http://www.eweek.com/c/a/Security/Spyware-Rootkit-Maker-Stops-Distribution/ (last visited Nov. 25, 2008).

[45] *See* Chris Williams, *ISP data deal with former 'spyware' boss triggers privacy fears*, THE REGISTER, Mar. 17, 2008, *available at* http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/print.html (last visited Nov. 25, 2008).

[46] *Id.*

[47] *Id.*

British Internet service providers TalkTalk and Virgin Media, to offer "a free consumer internet feature, Webwise, which ensures fewer irrelevant adverts and additional protection against malicious websites."[48] Williams quickly connected the announcement with the 2007 reports and posted a piece accusing Phorm and BT of cooperating to monitor.[49] By March, Phorm had admitted that it had undertaken a trial of its technology involving tens of thousands of users on the BT network with BT's participation, but without the knowledge of the users.[50] Privacy advocates reacted strongly against Phorm's monitoring of user connections since the revelation of the BT deal and of the secret trial, postponing any further use of Phorm on the BT network. But as of July 2008, BT planned to begin another trial of Phorm's system within a few weeks, though this time with an opt-in mechanism.[51]

Phorm attempts to allay privacy concerns by claiming that it does not store any personally identifying information or any specific information about the browsing habits of tracked users.[52] Instead, Phorm stores a persistent and unique, but randomly generated, Phorm identification number for each user, along with a list of the advertising categories triggered by each of the user's web requests.[53] So when a user requests a page about the Ford Expedition from ford.com, Phorm stores only the

---

[48] *See BT PLC, TalkTalk and Virgin Media Inc confirm exclusive agreements with Phorm*, Phorm, Inc. Feb. 14, 2008, *available at* http://www.phorm.com/about/launch_agreement.php (last visited Nov. 25, 2008).

[49] *See* Chris Williams, *ISP data deal with former 'spyware' boss triggers privacy fears*, THE REGISTER, Feb. 25, 2008, *available at* http://www.theregister.co.uk/2008/02/25/phorm_isp_advertising/ (last visited Nov. 25, 2008).

[50] *See* Chris Williams, *BT admits misleading customers over Phorm experiments*, THE REGISTER, Mar. 17, 2008, *available at* http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/print.html (last visited Nov. 25, 2008).

[51] *See* Philip Stafford, *BT to begin further trials of ad technology*, FT.com, July 16, 2008, *available at* http://www.ft.com/cms/s/0/34c59420-5356-11dd-8dd2-000077b07658.html (last visited Nov. 25, 2008).

[52] *See Privacy : Phorm : No Personal Information*, PHORM, INC., *available at* http://privacy.phorm.com/no_personal_info.php (last visited Oct. 20, 2008).

[53] *Id.*

fact that the user (identified only by the Phorm identification marker) requested a page indicating interest in an SUV (or perhaps even in a Ford Expedition) rather than the details of the content or the specific URL of the request.[54] Phorm uses these interest categories to serve targeted ads to customers in spots on web pages that it sells to content producers.[55] Further, Phorm installs machines inside its participating ISPs that inject its own cookie into every request, allowing it to track which user is connecting to which site and to identify each user to its targeted ad server.[56]

c. Pakistan: YouTube and AnchorFree

In February 2008, the Pakistani state told all Pakistani Internet service providers to block local access to a specific URL on the popular U.S.-based video-sharing service, YouTube.com.[57] The authorities ostensibly sought to block Pakistani citizens from viewing a video hosted on YouTube that was perceived to be too critical of Islam.[58] One of the Pakistani ISPs responded not just by blocking access to the single URL within Pakistan, but instead by blocking access to the entire YouTube.com site (and, in the process, blocking global access to YouTube.com for a short while through a network anomaly).[59]

During those few days that Pakistan was blocking YouTube.com locally, many Pakistanis continued to access YouTube.com by using tools to circumvent the filter, including Hotspot Shield, a free tool by a company called AnchorFree.[60]

---

[54] *Id.*

[55] *Id.*

[56] *See* Richard Clayton, *The Phorm "Webwise" System*, May 18, 2008, *available at* http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

[57] Posting of Sally Walkerman to OpenNet Initiative Blog, *available at* http://opennet.net/blog/2008/02/pakistan%E2%80%99s-internet-has-a-bad-weekend (Feb. 25, 2008 12:10 EST).

[58] *Id.*

[59] Posting of Ethan Zuckerman to My heart's in Accra, *available at* http://ethanzuckerman.com/blog/2008/02/25 (Feb. 25, 2008 15:41 EST).

[60] Sylvie Barak, *Pakistan Becomes VPN Routing Hot-spot*, THE INQUIRER, Feb. 26, 2008, *available at* http://www.theinquirer.net/gb/inquirer/news/2008/02/26/pakistan-becomes-vpn-routing (last visited Nov. 28, 2008).

AnchorFree describes its Hotspot Shield tool as: "Hotspot Shield creates a virtual private network (VPN) between your laptop or iPhone and our Internet gateway. This impenetrable tunnel prevents snoopers and hackers from viewing your email, instant messages, credit card information or anything else you send over a wireless network."[61]

But AnchorFree is, at its core, an advertising company which tracks the web browsing habits of its users.[62] What AnchorFree's description does not say is that AnchorFree makes money from the otherwise "free" tool by displaying ads to users within web pages. By using HotSpot Shield, users give AnchorFree complete access to all data exchanged while web browsing with the tool. AnchorFree provides an option to its users to remove the inserted banner ads and implies (but never explicitly says) that it does not monitor its users' traffic, but it nonetheless still has the ability to snoop on the data at any time. Thus, while the Pakistani state is watching its citizens' Internet traffic to block content it does not like, citizens are watching the blocked content by using a tool that circumvents Pakistan's filters. However, the circumvention tool itself could function as a monitoring tool, albeit likely for a different purpose.

3. Network Surveillance Data

Three sorts of data are vulnerable to surveillance on the network: (1) routing information, (2) the actual content of the data stream, and (3) contextual signatures. All Internet data packets must include the Internet Protocol (IP) address of the ultimate recipient. The Internet works more or less like a guided game of hot potato, with each packet of data getting passed through a series of intermediate routing computers that pass the packet on to another router closer to the end destination. In order to perform this function, every router along the way must include the address of the ultimate

---

[61] AnchorFree Inc., *AnchorFree History*, *available at* http://anchorfree.com/downloads/hotspot-shield/ (last visited Oct. 15, 2008).

[62] AnchorFree, Inc., *How it Works*, *available at* http://anchorfree.com/advertisers-agencies/how-it-works/ (last visited Nov. 11, 2008).

destination. Most data packets, all using the TCP protocol, including all web and email traffic, also include the IP address of the sender, such that data can be sent back along the same channel.

Users can hide routing information on the network by using a proxy that forwards communications between a client and a server. Using a proxy allows a user to include the proxy's address as the recipient in the packet routing data and move the ultimate recipient data into the content of the packet proper. The proxy receives the packet, looks inside the packet content for the ultimate recipient, and forwards the packet on to the recipient. Routers between the sender and proxy that look at the packet routing data see only that the client is sending a packet to the proxy. Likewise, routers between the proxy and the recipient that look at the packet routing data see only that the proxy is sending a packet to the recipient. No single router, other than the proxy itself, sees that the sender is communicating directly with the recipient.

In addition to these routing data, the packets contain the content of the data. The content includes both protocol-specific data and the content proper of the communication. The protocol-specific data includes data about the URL requested, the referring URL, the user agent, and so on for web requests as well as data that describe the originating email server, the from email address, the date and so on for emails. The content proper of the communication includes, but is not limited to, any data submitted to web server forms, any web pages retrieved, any emails sent or received, and any videos watched or songs downloaded. Any communications of any significant size are divided into separate packets for travel across the network, making it more expensive but not impossible for routers along the way to recreate the entire content objects (whole web pages, videos, and so forth) than to snoop on the routing information of a given packet or to look for simple patterns like keywords in a single packet.

Users can hide the content of their communications on the network by encrypting their messages, preventing anyone other than the sender or recipient from monitoring the data in

between the end-points. Encryption is most effective when it is applied end-to-end, so that the entire stream of data from the client to the server is encrypted, allowing no one on the network between the sender and the receiver from reading the content. Secure web (HTTPS) and email (SMTPS, IMAPS, POPS) protocols, when properly configured, are examples of this sort of end-to-end encryption. End-to-end encryption has to be negotiated by both the client and the server; however, many servers do not support encrypted communication, or only do so for some subset of content or functionality. In these cases, a user can connect through a proxy to encrypt the data from the client to the proxy. But such encrypting proxies still have unencrypted channels that enable them to talk to servers that do not support encryption, such that the proxied content remains readable to some routers on the network.

Communications that are both encrypted and proxied can hide both the routing information for and the content of a communication from the network between the client and the proxy. But even proxied and encrypted data leaks some information about the communication between the parties: the timing, number, and size of the packets as well as the fact that the communication is proxied and encrypted give away information about the transaction. In some cases, the mere fact that the data is encrypted prompts suspicions about the users and gives rise to further surveillance. Different sorts of traffic generate different signatures of packet size and timing that can allow easy identification of the nature of the communication.[63]

4. Network Surveillance and the Problem of Trust

The number of links on the Internet is the same as the sum of the number of clients, servers, and routers, roughly speaking,

---

[63] *See* Charles Wright, Lucas Ballard, Scott Coulls, Fabian Monrose, & Gerald Masson, *Spot Me if You Can: Recovering Spoken Phrases in Encrypted VoIP Conversations* (forthcoming, Proceedings of IEEE Symposium on Security and Privacy, May, 2008); *see also* Charles Wright, Lucas Ballard, Fabian Monrose & Gerald Masson, *Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?* (Proceedings of the 16th USENIX Security Symposium, Boston, Aug. 2007) (for discussions of traffic analysis and data leakage).

all the computers hooked up to this global network of networks. If monitoring the network required monitoring each one of those hundreds of millions of links, network monitoring on a large scale would be prohibitively expensive for even the most well-funded law enforcement or intelligence agencies. In practice, all Internet traffic flows through a much smaller number of routers, and those routers are controlled by an even smaller number of Autonomous Systems (AS) that agree to use the Border Gateway Protocol (BGP) to direct the traffic amongst themselves. These AS's are generally commercial ISPs, though they can also be managed by companies, governments, universities and other large organizations. There are fewer than a hundred thousand of these AS's in the world. The vast majority of Internet traffic flows through a much smaller number of those AS's.[64] Traffic within a given country generally stays on AS's located within that country, with some exceptions for countries with very little Internet usage. For a combination of technical, business, and policy reasons, a disproportionate amount of global Internet traffic flows through a few very large AS's in the United States, including most traffic between Europe and Asia.[65]

This topology of the Internet has a few different implications for the actors trusted with access to Internet data. The first is that a large majority of users need to access the Internet through an AS, usually a commercial ISP. These users are therefore vulnerable to surveillance by that AS itself. The second is that there is a relatively small number of these AS's within any given country, so monitoring all of the network traffic in a given country is a relatively manageable task; the state simply needs to require a small number of AS's to monitor their networks. This applies doubly for international Internet traffic, which is controlled by an even smaller number of AS's that are disproportionately located in the United States. Thus

---

[64] *See* BGP: The Border Gateway Protocol Advanced Internet Routing Resources, *Global Internet Exchange Points / BGP Peering Points / IXP*, *available at* http://www.bgp4.as/internet-exchanges (last visited Oct. 9, 2008).

[65] Cooperative Association for Internet Data Analysis, *IPv4 Internet Topology Report as Internet Graph*, *available at* http://www.caida.org/research/topology/as_core_network/ (last visited on Oct. 9, 2008).

monitoring international traffic within a given country requires the participation of even fewer AS's. The United States is capable of monitoring a large portion of international Internet traffic through a few of its AS's, including even traffic flowing between two non-U.S. countries.[66]

If a citizen wishes to hide her data on the network, her most likely strategy would be to move her trust around. In the process, though, the user must trust one or more actors with his or her data. One common approach to sharing trust in this manner is to use the Tor system to defend oneself against traffic analysis. In so doing, however, a user relies to a certain extent upon others on the network who are operating parts of the Tor network and whose machines relay information to others on the network.[67] Likewise, a user who tries to get around Phorm surveillance of her local ISP connection has only a few choices of ISPs in the United Kingdom, most of which have been reported to be considering adding Phorm monitoring to their networks. The user may choose to stay on the possibly monitored local network, but use a service like Relakks to proxy and encrypt her data as it travels through the local, Phorm monitoring, ISP. The user will avoid Phorm monitoring in the process, but at the cost of trusting not only Relakks but also the Swedish ISP through which Relakks talks to the Internet *and* the Swedish government that has legislated access to the data flowing through all Swedish ISPs. Her local ISP will still have the ability to tell that she is proxying and encrypting all of her data through a third party, which fact itself might prove suspicious if queried by a law enforcement. Finally, the user's data is vulnerable to network monitoring at any point along which it travels, from her local ISP to the server's ISP to any ISPs between that carry the data. Even setting aside the monitoring possibilities on her local ISP, a large portion of her data is likely to travel outside of Europe and is there likely to flow through one of a few U.S. ISPs that process a disproportionate share of international Internet traffic. The point is that, in evading

---

[66] *Id.*

[67] *See* http://www.torproject.org/ (last visited Oct. 8, 2008).

traffic analysis and other forms of online surveillance, a user will have to trust someone—or a series of people—to some extent in order to communicate via the network.

B. Server Surveillance

Surveillance also takes place commonly at the server level. In this taxonomy, servers include the computers that large corporations use to provide access to online services to consumers. Far more data are likely collected each day, by more parties, at the server level than through the network surveillance examples described above. But rarely do states directly have access to these data; a law enforcement or intelligence official would have to obtain it through the corporate or other institutional data-holder.

1. The Fuss About Google

Americans have begun to worry that perhaps Google's engineers know too much about what we do. To address these worries, Google has published a series of videos on YouTube that explain the privacy implications of the data collected by its search engine. A spokeswoman on one of these videos is named Ms. Ohye, a professional, reassuring-sounding support engineer. In the video, she explains what sorts of data Google collects and, implicitly, why users should not be particularly concerned about the data collection. Ms. Ohye says:

> To improve our search results, as well as maintain security and prevent fraud, we remember some basic information about searches. Without this information, our search engine wouldn't work as well as it does or be as secure. . . . We're able to [replace 'carss' with 'cars'] because we've studied search queries in our logs and found that when people type in 'carss' they often really mean 'cars.' . . . Only your provider can directly match you with your IP address. . . . What a cookie doesn't tell Google is personal stuff about you like where you live and what your phone number is. . . . In the same way that a store keeps a receipt of your purchases, Google keeps a type of receipt of

> your visit called a log. . . . As you can see, logs don't contain any truly personal information about you.[68]

User search data does help in the way Google says it does ("improve our search results," "maintain security," and "prevent fraud"). Ms. Ohye's descriptions of the way Google collects data are true in a technical sense. But the importance of data is determined by the larger world in which it lives—by the other data to which it connects. So when Ms. Ohye asserts that a cookie does not tell Google "personal stuff about you like where you live,"[69] this is only true in the sense that the cookie that contains your driver's license number does not tell the police where you live. However, even though the cookie itself is just a random string of letters, as with a driver's license number, it can indeed be used to lookup personal information "like where you live."

For example, the cookie might connect, reasonably well, all searches performed by a single person. Many people search for their own names and addresses at some point (if for no other reason than to see their houses in Google Maps). The cookie might connect those two searches to the same (otherwise pseudonymous) person, thus potentially identifying the name and address of the person behind the random gibberish of a particular cookie. This method of identification is not perfect, but researchers have consistently shown the ability to crack the identity of individual users in these kinds of data collections with anonymous but individually unique identifiers, most dramatically on supposedly anonymized data sets released by AOL and Netflix.[70]

---

[68] Google, Inc., Google Search Privacy: Plain and Simple, *available at* http://www.youtube.com/watch?v=kLgJYBRzUXY (Aug. 8, 2007).

[69] *Id.*

[70] *See* Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000 (last visited Nov. 28, 2008); Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Datasets, *How To Break Anonymity of the Netflix Prize Dataset*, *available at* http://arxiv.org/abs/cs/0610105 (last visited Nov. 28, 2008). *See also* Christopher Soghoian, *The Problem of Anonymous Vanity Searches*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 299, 300 (2007).

In fact, it is likely that this collection of search terms, IP addresses, and cookies represents one of the largest single collections of personal data on or offline. Google may or may not choose to do the work necessary to translate its collection of search data into a database of personally identifiable data, but it does have the data and the ability to query personal data out of the collection at any time if it chooses. Even if Google's staff never chooses to access these data, an intruder or disgruntled employee may query the data himself, or a state may demand access to it, with the force of law behind its request. And even assuming perfect security, Google is still subject to many sorts of government requests, as demonstrated by the success of the recent subpoena by Viacom for Google's entire retained history of which users watched which YouTube videos.[71]

One of the key Google services, AdWords, is a contextual online advertising system that displays ads on Google and its partner search sites, major content sites like the *New York Times*, and, through the AdSense program, on a huge number of small content providers like blogs. Through AdWords, Google targets ads to relevant consumers by displaying ads based on the current interests of a user. For ads on search pages, it displays ads related to the keywords entered by the user for the given search. For example, a user who searches for "digital camera" will see ads targeted to people interested in digital cameras. For ads on content providers, the system displays ads relevant to the keywords present in the content itself. So an article on digital cameras on a blog will draw AdWords ads about digital cameras. Advertisers bid for the right to advertise on desired keywords. An advertiser who wants to advertise to users interested in digital cameras has to win a continuous action for the term "digital camera" (or one of a host of related terms). At any given time, the ads that appear with a given term are those whose owners have made the highest bids for a single click on an ad that appears alongside a search (or a page of relevant content) for the bid keyword.

---

[71] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, N.Y. TIMES, July 4, 2008, *available at* http://www.nytimes.com/2008/07/04/technology/04youtube.html (last visited Nov. 28, 2008).

Google watches consumers click on ads through its AdWords system and watches the advertisers through AdWords auctions that determine the value of advertising topics. Content providers watch the value of those advertising topics to determine which sorts of content to publish. The advertisers use the Adwords system as a stateless form of market research to target consumers without knowing anything about them. Content providers watch consumers to determine which sorts of content generate the most interest. The combined effect of these activities is to create a system of surveillance that collectively monitors what topics content producers are writing about, what topics users are searching for, and what the value of those topics (or rather the users who are reading about those topics) is to advertisers.

All of the monitoring that happens within this system of surveillance happens in real time. Google adjusts the placement of ads in real time according to the current results of the auction, content providers watch the profitability of their content in real time and make adjustments to attract more ad clicking customers, and advertisers adjust their bids and update their ads in real time to attract more users. The effect of the system is continuous but stateless market research that is constantly adjusting to the current interests of users rather than the historical interests over time tracked by user profiling organizations like comScore, Phorm, and NebuAd.

2. Server Surveillance Data

A server has access only to data that is sent directly to it over the network, which consists of the client address, the time of the communication, and the protocol-specific request (in the case of an http server, the URL, referrer, user agent, and any cookies). The server also likely captures the content explicitly submitted by the user, including names, addresses, credit card numbers, health problems, sexual proclivities, and so on. All of these data, other than the client and the time of the transaction, may be encrypted while traveling over the network, giving the end server access to some data that is not available on the network. For web servers, the protocol data may include

cookies, which are often used to assign to the requesting user a pseudonymous identity that remains the same between separate requests.

3. Server Surveillance Trust

People voluntarily, if not exactly knowingly, submit vast amounts of data to Internet servers. When one pauses to think about it, one may be aware that one is submitting names, addresses, and credit card numbers to Amazon when buying a new book, personal email to Microsoft through the popular free service Hotmail, movie preferences to Netflix when renting videos, medical information when using online personal health services, and all manner of personal information when connecting to others through social networks or online dating services.[72] What determines the risk of privacy intrusions is not so much the data itself as what the actors controlling the servers do with the data, with whom they share it, and how the data are later combined with other data. So, for some users, allowing a company to collect a credit card number to execute a purchase is fine, but using that same credit card number to request data about the user's purchase history from the credit card company in order to target advertising to him or her is not fine. Likewise, it may be fine for Microsoft to collect personal emails through Hotmail, but it becomes a concern if Microsoft were to sell its users' email content to a consumer research company. A consumer may be pleased that Netflix uses video preference information for its own recommendation engine, but many users would be uncomfortable if they found out that Netflix was combining its users' video rental history with (even public) information from users' Bebo social networking pages to make

---

[72] In a further twist to this story, users sometimes seek to protect communications by using supposedly secure services, only to have those service providers turn over data to law enforcement officials. *See, e.g.*, http://blog.wired.com/27bstroke6/files/steroids.source.prod_affiliate.25.pdf (last visited Nov. 28, 2008). One prominent case involved the Canadian email provider Hushmail, which, according to court documents, assisted U.S. law enforcement authorities by turning over emails relating to the activities of suspected criminals in the United States. *Id.*

video recommendations.

All of these different possible uses of data represent networks of trust which the user must evaluate. The Google story provides an example of the complexity and confusion surrounding these issues of trust. Studies of users of all ages, but especially young people, suggest that few have a clear idea about how data is collected, who has access to it, and what is done with it.[73] The potential of Google's vast store of user data creates a serious risk of disclosure throughout this network of trust, regardless of Google's intentions.

Sometimes the risk is more than theoretical. Over the past several years, many users around the world have come to rely upon the Skype service for voice over Internet protocol calling and online chat. The service has often been touted as among the most secure ways for dissidents and activists to communicate.[74] However, Internet researcher Nart Villeneuve found that "[t]he full text chat messages of TOM-Skype users, along with Skype users who have communicated with TOM-Skype users, are regularly scanned for sensitive keywords, and if present, the resulting data are uploaded and stored on servers in China."[75] In other words, while Internet activists were trusting Skype with their communications, keyword monitoring of their chat in China directly resulted in the potential for state surveillance of their supposedly private communications.[76]

---

[73] PALFREY & GASSER, *supra* note 4, at 39-82.

[74] *See* Robert Amsterdam, *Technology's Threat to Human Rights and Free Speech*, (Oct. 31, 2008), *available at* http://www.robertamsterdam.com/2008/10/technologys_threat_to_human_ri.htm (last visited Nov. 25, 2008).

[75] NART VILLENEUVE, INFORMATION WARFARE MONITOR/ ONI ASIA JOINT REPORT, BREACHING TRUST: AN ANALYSIS OF SURVEILLANCE AND SECURITY PRACTICES ON CHINA'S TOM-SKYPE PLATFORM 4 (Oct. 1, 2008), *available at* http://www.infowar-monitor.net/breachingtrust.pdf (last visited Nov. 28, 2008).

[76] John Markoff, *Surveillance of Skype Messages Found in China*, N.Y. TIMES, Oct. 2, 2008, at C1, *available at* http://www.nytimes.com/2008/10/02/technology/internet/02skype.html (last visited Nov. 28, 2008).

4. Server Surveillance Implications

Google's current policy is to keep a log of each search query with a complete IP address for eighteen months and then remove a portion of the IP address to make it harder to resolve back to a specific user.[77] Data retention rules, such as the European Union Data Retention Directive, mean that a given firm may be—or perceive itself to be—compelled to retain more information about users for greater periods of time. The scrubbing of server data provides only limited protection against identification since the combination of search terms over time can still be used to resolve the data to individual users. The combination of technological change, rules and practices of data retention, and individual willingness to share private information with firms gives rise to a growing potential for data related problems at the server level.

C. Client Surveillance

1. Government Surveillance at the Client Level

Governments have various levels of control over and access to the data collected by client side software, but they also use this software to directly collect data in certain instances. The uses of client side software can be difficult to uncover, but the practice of using it is well-known. For example, United States court documents reveal that in 2007 the U.S. Drug Enforcement Agency (DEA) installed a keylogger on a suspect's machine to capture the encryption keys necessary to read the suspect's PGP (Pretty Good Privacy) encrypted email.[78] In fact, the alleged New Jersey organized crime boss, Nicholas Scarfo, was caught through the FBI's use of a keylogger on a personal computer.[79]

---

[77] Posting of Chris Soghoian to CNET news blog, *available at* http://news.cnet.com/8301-13739_3-10038963-46.html (Sept. 11, 2008, 7:40 PDT).

[78] Declan McCullagh, Feds Use Keylogger to Thwart PGP, Hushmail, CNET News Blog, (July 10, 2007), *available at* http://news.cnet.com/8301-10784_3-9741357-7.html (last visited Nov. 28, 2008).

[79] Electronic Privacy Information Center, United States v. Scarfo, Criminal No. 00-404 (D.N.J.), *available at* http://epic.org/crypto/scarfo.html (last visited Oct. 12, 2008).

Some major anti-virus companies have received and complied with court orders to ignore the presence of government agency spyware when scanning for viruses.[80] Similarly, there is evidence that the German police are aggressively pursuing the use of client side software to calls placed on the Skype Internet telephone service.[81] The software used in both cases includes features identical to those in malware, including remote installation via a trojan or virus, remote control and data reporting, and stealth features (and policies) that hide the software from the user.

A variety of companies make keyboard logging devices that are hardware, rather than software. These devices tend to take the form of small plugs that sit between the USB plug of the logged keyboard and the USB plug of the logged computer. The devices record every key pressed on the keyboard and therefore can be used to capture passwords, emails, typed documents, and any such information entered on the keyboard. These devices are much easier to install than software keyloggers, so long as the installer has physical access to the machine, and they are impossible to detect via anti-virus software. A company called KeyCarbon distributes a PCI keylogger.[82] As a PCI card, this device is attached to the motherboard inside the computer case, giving it all of the advantages of a USB keylogger (though requiring a few minutes instead of a few seconds to install) but making the device much more difficult to detect via visual inspection.[83] The only way to detect this device is physically to open the computer case and then look inside the box in the right

---

[80] Posting of Declan McCullagh & Anne Broache to CNET News blog, *available at* http://news.cnet.com/Will-security-firms-detect-police-spyware/2100-7348_3-6197020.html (July 17, 2007, 9:40 PDT).

[81] Posting of Louis Charbonneau to Reuters News Blog, *available at* http://www/reuters.com/article/technologynews/idusl21173920071122 (Nov. 23, 2007, 12:28 EST); *see also* posting of Kim Zetter to Wired Blog Network, *available at* http://blog.wired.com/27bstroke6/2008/01/leaked-document.html (Jan. 29, 2008, 16:10 EST).

[82] KeyCarbon Computer Security Hardware, *available at* http://www.keycarbon.com/products/keycarbon_laptop/overview/ (last visited Oct. 13, 2008).

[83] *Id.*

place.[84]

2. Market Research

ComScore Incorporated is one of several large companies that collect data about Internet users for market research. ComScore collects the entire web browsing stream, including encrypted requests, from the two million members of its "consumer panel."[85] It claims to try to avoid capturing data like usernames, passwords, and credit card numbers, but actively collects personal information that directly identifies the owner of the web browsing data.[86] ComScore touts the ability to connect this online data to a variety of other consumer databases, including supermarket purchases and automobile registrations.[87] It has admitted in the past to using its monitoring data to look up information in its panel members' online banking accounts to verify the household incomes reported in surveys.[88]

ComScore recruits these panel members through a combination of sweepstakes, network performance improvement tools, claims of anti-malware protection, and an appeal to those who seek to improve the efficiency of the Internet.[89] ComScore discloses to the panel members that the software is monitoring their web browsing activities, but it also keeps a strong separation between itself and the operations that collect the data, currently OpinionSquare and PermissionResearch, by not directly naming the tools or the organizations that operate them anywhere on comScore.com or even in its SEC annual report filing, and it has had to recreate those operations at least once to

---

[84] *Id.*

[85] comScore, Inc., comScore Methodology, *available at* http://www.comscore.com/method/method.asp (last visited Oct. 13, 2008).

[86] *Id.*

[87] *Id.*

[88] Posting of Evan Hansen to CNET News Blog, *available at* http://www.news.com/Net-privacy-and-the-myth-of-self-regulation/2010-1071_3-281580.html (Oct. 16, 2001, 4:00 PDT).

[89] *See* comScore, *supra* note 85.

evade detection by anti-spyware tools.[90] ComScore sells this vast trove of data, estimated by comScore at 28 terabytes collected per month in 2007, as market research to many of the largest companies in the world.[91] ComScore is far from alone in collecting vast amounts of data about individuals for the purposes of greasing the wheels of commerce, online and off; ChoicePoint, its parent company LexisNexis, and many others are in the business of serving as "data brokers."[92]

3. Malware and Antivirus Software

Though the furthest cry from the man in the van with headphones, malware installed on an individual's computer can perform some of the most intrusive surveillance possible using today's technology. A motley assortment of computer programs and related systems called bots, virus, worms, trojans, and other malware infect up to twenty-five percent of all computers connected to the Internet.[93] All of these malware programs are surveillance devices: they have complete access to all data entering, leaving, or residing on the client computer. Malware programs generally use their access to user data to perform a variety of illicit activities including sending spam, committing click fraud, attacking other computers, and stealing financial or other identifying information from the client. The direct impact of most of these activities on any given infected user is relatively small—outgoing spam only costs the user bandwidth and even

---

[90] Hoovers, United States Securities and Exchange Commission Form 10-K Annual Report for comScore, Inc., *available at* http://www.hoovers.com/free/co/secdoc.xhtml?ID=113840&ipage=5792564 (filed on Mar. 11, 2008); *see also* posting of Stefanie Olsen to CNET News Blog, *available at* http://news.cnet.com/ComScore-Spyware-or-researchware/2100-1032_3-5494004.html (Dec. 20, 2004, 4:00 PST).

[91] *See* Tom Taulli, *comScore Busts a Move*, The Motley Fool, June 28, 2007, *available at* http://www.fool.com/investing/high-growth/2007/06/28/comscore-busts-a-move.aspx (last visited Nov. 11, 2008).

[92] Martin H. Bosworth, *Lexis-Nexis Parent to Buy Choicepoint*, (Feb. 23, 2008), *available at* http://www.consumeraffairs.com/news04/2008/02/choicepoint_sale.html (last visited Nov. 30, 2008).

[93] Tim Weber, Business Editor, BBC News Online, *Criminals may overwhelm the web*, (Jan. 25, 2007), *available at* http://news.bbc.co.uk/1/hi/business/6298641.stm (last visited Nov. 28, 2008).

credit card theft is generally insured by the credit card company.

These malware programs have the potential to exploit more directly the vast trove of personal data stored on the vast number of infected machines, as demonstrated by the Sircam worm in 2001.[94] Like many worms of its era, the Sircam worm propagated by sending a copy of itself to every email address in each infected computer's address book.[95] Unlike other worms, however, Sircam tried to fool its targets into opening the infecting payload by attaching a trojan to a document picked randomly from the victim's own computer.[96]

The primary effect of the worm, other than clogging up the network, was to send the randomly chosen private files of over a million people to a list of their friends, families, colleagues, and digital acquaintances.[97] The *New York Times*, for instance, reported receiving a travel diary, a document about a father's will, and a memo from a real estate branch manager that "offers colleagues 'Objectives For The Year 2000,' the first of which is, 'Positive attitude at all times.'"[98] Others reported receiving "memos, CVs, job listings, diary entries, expense forms and complaint letters."[99] For many, the disclosure of these documents, particularly to friends and colleagues, represented serious breaches of privacy with significant personal repercussions.

Most malware, circa 2008, tries to hide itself from detection. It tends to avoid heavy-handed tactics like those of the Sircam worm. Modern malware largely restricts itself to hijacking the

---

[94] Symantec, w32sircamworm@mm_2007, *available at* http://www.symantec.com/security_response/writeup.jsp?docid=2001-071720-1640-99&tabid=2 (last visited Oct. 13, 2008).

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] Richard Meislin, Compressed Data: A Virus, Yes, but One That Brings Interesting Things, N.Y. TIMES, (July 30, 2001), *available at* http://query.nytimes.com/gst/fullpage.html?res=9C00EEDA103DF933A05754C0A9679C8B63 (last visited Nov. 28, 2008).

[99] Mark Ward, Technology Correspondent, BBC News Online, *Sircam virus steals files*, (July 24, 2001), *available at* http://news.bbc.co.uk/1/hi/sci/tech/1454155.stm (last visited Nov. 28, 2008).

user's identity to send spam or commit click fraud or to stealing profit-generating information like credit card numbers. The Sircam story, however, demonstrates that these forms of malware have the capability to breach the privacy of millions of infected users in much more serious ways than stealing credit card numbers. The collection of malware-infected computers as a whole represents the single largest surveillance device on the Internet, capable of collecting and processing the personal data of probably hundreds of millions of computers.

Viruses, too, can collect personal information. On Christmas Day 2007, the SANS Internet Storm Center received a report from a user who had found trojan malware on a new digital photo frame purchased from a large retailer, Sam's Club.[100] Within a week, two more readers of the SANS blog reported finding the same virus on other digital photo frames; and, within a couple of weeks, readers reported similar viruses on a wide array of different consumer devices that acted as USB storage devices, including MP3 players, portable hard drives, and video cameras.[101] The malware found on many of these devices was the MocMex trojan horse, a powerful piece of malware capable of hiding itself from a variety of anti-virus tools.[102]

To protect from viruses, bots, worms, and other such malware, millions of computer users install anti-virus systems on all client computers. But this anti-virus software is itself highly intrusive, operating at the lowest levels of the operating system, incurring significant performance penalties, and attempting to avoid the notice of malware (which are themselves trying to detect the anti-virus systems to disable them). The extensive access given to anti-virus software gives it the capability to do the same sorts of harm that a piece of malware

---

[100] Digital Hitchhikers, *available at* http://isc.sans.org/diary.html?storyid=3787 (Dec. 25, 2007, 23:24 UTC).

[101] Digital Hitchhikers, Part Four, *available at* http://isc.sans.org/diary.html?storyid=3892 (Jan. 28, 2008, 10:37 UTC).

[102] Deborah Gage, *Virus from China the Gift that Keeps on Giving*, SAN FRANCISCO CHRONICLE, Feb. 15, 2008, at C-1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/15/BU47V0VOH.DTL&type=printable (last visited Nov. 28, 2008).

can do, including both stealing data from and disabling the host computer. The difference between a legitimate anti-virus tool and malware is the trustworthiness of the software distributor. Most people trust that Symantec—the provider of a common type of anti-virus software—is only using its complete access to protect the user's own computer, while few people trust that a malware developer or operator will not abuse its access. Internet users have little choice but to trust someone with their data.

4. Client Surveillance Data Implications

Client side surveillance provides the most complete access to user data. As such, surveillance techniques by the state that either gain access at the client level or obtain data collected by others will yield the most detailed picture of the activities of a suspect. It is for this reason, of course, that law enforcement officials often seize laptops and turn them over to a computer forensics expert to review.

Virtually every bit of data stored, sent, received, viewed, played, or typed on a computer is vulnerable to client-side surveillance. The only data that is potentially not accessible is encrypted data that is never accessed during the period of surveillance. Everything else on a computer is available to a client surveillance tool. The primary limiting factor is simply what the tool developers choose to target with their tools. Malware mostly targets various sorts of easily monetized data, including email addresses, credit card numbers, bank account information and login credentials, and game and other software keys. The most sophisticated anti-virus tools monitor all data stored on and transmitted to the computer, checking all data for malware signatures, but not keyboard or screen activity. Market research tools like comScore typically monitor all network traffic, whether encrypted or not, but not stored data or keyboard or screen activity. Workplace and family monitoring tools usually monitor keystrokes and sometimes screenshots of the minute to minute (or even second to second) activity on the computer screen but not stored or network data.

Client side surveillance tools are often designed not to track

certain types of data in order to provide a clearer, more focused set of data to the party carrying out the surveillance. In fact, the biggest problem of surveillance on the client side is often dealing with the sheer amount of data. For example, even one screenshot a minute on a single computer can generate a daunting amount of data. This problem is magnified when applied over a large set of monitored clients. Botnets (networks of malware-infected computers controlled from a single point) only search for a limited set of data, like credit card numbers, which can easily be monetized, presumably because of the difficulty (and, therefore, unprofitability) of sifting through the vast trove of other sorts of data on infected computers. Likewise, a primary challenge for corporate anti-virus systems that must manage entire networks of clients is to manage the resulting flood of data.

Any client side program has at least the *potential* to access every sort of data that resides on or passes through the computer. In fact, even non-surveillance oriented programs (screen savers, games, chat programs, and so on) have this access to the computer once they have been installed.[103] This same access applies to most hardware devices installed on the computer as well. Any device that has access to a shared channel—such as the USB, PCI, or IDE channels—has the ability to monitor all data on that bus directly, and any device that requires an operating system driver can use that driver to access the breadth of data available on the client computer. Even devices that do not directly have the ability to access a shared bus or run drivers may have the ability to infect clients with malware.

IV. Implications of the Digital Difference

The fact that digital technologies afford this increased level of surveillance is not inherently bad. There are, in fact, many

[103] Most modern operating systems have some level of access control that is intended to prevent ordinary programs from having complete access to the data on the computer. In practice, it is almost always possible to exploit a vulnerability that breaks through the access control system to give the client complete access to the system.

good reasons to exercise this power. From the perspective of law enforcement, these multiple modes of digital surveillance can lead to new and better ways to prevent crimes and to bring criminals to justice. And though the fear of aggregating these many sets of data, held in many hands, is true in concept, the reality is that it is technically difficult to pull disparate data sets together in a way that is helpful for purposes of surveillance.[104]

The issue raised by these changes in technologies and their usage is whether individual data-sharing practices and the safeguards for civil liberties are keeping up with the changes.[105] Of the many things that have changed in the digital era, the manner in which surveillance can be carried out by the state is high on the list of the more dramatic types of changes. Compare traditional surveillance to Internet-era surveillance and the differences become plain. In traditional surveillance, the law enforcement official primarily focuses on known targets and has access largely to live communications and imperfect records of past interactions. The data that can be tracked are mostly in rivers (such as tapping a phone conversation) rather than in the form of oceans (which might later be searched).

In the digital age, law enforcement officials have many more means of surveillance than in the past. (Of course, there are reasons to celebrate this fact in the interests of public security.) Law enforcement officials have the opportunity to

---

[104] Simson L. Garfinkel, *Information of the World, Unite!*, SCI. AM., 82-5 Sept. 2008.

[105] There is interesting literature related to privacy in a digital age and how we might reconceptualize it in light of recent changes in technology, which often expands the frame of a discussion such as the one here in this paper. As one example, Julie Cohen has recently written an article on the information privacy law project and its intersection with the Fourth Amendment doctrine. Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181 (2008). In this article, Cohen notes that privacy and technology literature focuses on informational privacy, but that spatial privacy is a relevant concept often overlooked in recent discourse. *Id.* at 183, 189-90. Cohen suggests that the spatial dimension of privacy is important, in light of internet usage, as "online conduct and online surveillance are experienced spatially." *Id.* at 194. When online activities are conceptualized as something one does in a "networked space," this "zone of personal space" is a meaningful and useful concept for privacy discourse. *Id.* at 195. Recognizing that online activities exist in a networked space also suggests that individual behavior changes within that space (for better or worse) in response to the awareness that one is being surveilled within that space. *Id.* at 195-96.

either focus on a known target or look for patterns across a network that might give rise to suspicion. Both rivers and oceans of information are available, depending upon the period during which data are retained in any given situation. Law enforcement officials have access to past, stored communications, which may or may not have seemed relevant during the initial surveillance. Data could be collected, placed in a large database, and later sorted, at much greater speeds and at lower costs than ever before. In addition, past actions can be recreated much more effectively based on third-party data collected in the course of everyday interactions. Profiles can be sewn together across data sources to create a more comprehensive profile of an individual or a pre-determined "type" of person.

The practice of non-targeted Internet surveillance is also rendered much easier in the digital era. A law enforcement official might establish a "driftnet" to capture all traffic through critical points in the network, much as the NSA is believed to have done through the black box in a closet at AT&T. Automated filtering and processing of traffic is far cheaper and faster than ever before, such that a non-targeted search might yield patterns or point to suspicious practices. This form of searching requires less human involvement than in the past. A person is needed for coding the system, setting filters, and reviewing results—but not for reviewing everything as it goes past. Such non-targeted surveillance might enable law enforcement officials to identify persons matching a predefined profile, to identify unusual patterns not predefined, or to record networks for unknown, future searching purposes.

In the digital era, governments also collect and review information about individuals for purposes not related to the traditional mode of law enforcement. For instance, government officials collect information for the purpose of record-matching between different government databases in order to ensure that welfare recipients are not perpetrating fraud.[106] The United

---

[106] *See* Virginia Eubanks, *Technologies of Citizenship: Surveillance and Political Learning in the Welfare System*, *in* SURVEILLANCE AND SECURITY: TECHNOLOGICAL POLITICS AND POWER IN EVERYDAY LIFE 89, (Torin Monihan, ed., 2006). *See also* JOHN

States Census Bureau collects highly sensitive personal data—such as income, race, ethnicity, physical handicap, and so forth—as part of its American Community Survey from a small sample of the population; recipients are told that they are "required by law" (Title 13 of the United States Code) to respond.[107] The handwritten data entered by citizens are then keyed into government databases.[108]

At the same time, most people are not able to keep up with all the changes in the technology that encode these data and otherwise enable this surveillance to happen in so many different ways. Through our research with young people, for instance, we found they were almost universally surprised to learn of the extent to which information was collected about them by third parties and the extent to which that information could be monitored, stored, and later searched.[109] As the possibilities for law enforcement to practice surveillance in concert with private third parties grow each year, public awareness of these practices is not keeping pace.

V. THE PUBLIC, THE PRIVATE, AND THE REASONABLE

Two primary concerns arise out of this fast-changing state of affairs. The first is about the convergence of the public and the private. The related concern is whether citizens are able to make reasonable choices about how they lead lives mediated by these technologies and what the consequences of those choices might be with respect to what the state can come to know about them.[110]

GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001).

[107] Census.gov, ACS Congressional Tool Kit 1, *available at* http://www.census.gov/acs/www/SBasics/congress_toolkit/ACS%20Tool%20Kit.pdf (last visited Oct. 18, 2008); *see also* Census.gov, American Community Survey (ACS), *available at* http://www.census.gov/acs/www/index.html (last visited Oct. 18, 2008).

[108] *See* Census.gov, About the Data (Methodology): Data Collection & Processing, *available at* http://www.census.gov/acs/www/AdvMeth/CollProc/CollProc1.htm (last visited Oct. 18, 2008).

[109] PALFREY & GASSER, *supra* note 4, at 39-82.

[110] There are, to be sure, other fears to which this set of facts might give rise, such as the overall suite of powers granted to law enforcement authorities to carry out network

A. Shifting Meanings of Public and Private

There are two meanings of "public" and "private" that have salience in the context of surveillance. The first is from the perspective of the person who is observing someone else. Is this observer a public actor? And is this public actor relying solely upon data collected by him or herself, or instead relying upon data collected by private actors? Second, this distinction matters from the perspective of the person who is being observed. The issues involved in each one are different from the other.

1. The Perspective of the Observer

The Fourth Amendment regulates the conduct of state actors where that conduct might violate an individual's reasonable expectation of privacy.[111] From the observer's perspective, much turns on whether the actor falls into the category of a state actor—for shorthand, here, representing the "public"—and whether that state actor carries out the surveillance directly. In this sense, the meaning of the "public" makes perfect sense: if the actor is a state actor and is carrying out the surveillance directly on a known target, then the traditional Fourth Amendment analysis follows. This paper does not dwell on this topic since there is a rich body of scholarship on the question of when and whether a warrant should issue.[112]

The issue addressed in this paper focuses on when the observer is a public actor and when the relevant data have been gathered by a *private* actor. The question asked near the threshold of a Fourth Amendment analysis does not have to do with the data involved or how those data were initially gathered. Vastly more data are now gathered through digital means, at

---

surveillance. Orin S. Kerr takes up these general issues and debunks several of the common myths on this related topic. Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607 (2003).

[111] *See* Smith v. Maryland, 442 U.S. 735, 739 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[112] *See, e.g.*, William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881 (1991).

the network, server, and client levels. So long as the collection of the data is performed by the private party, and the public party obtains the information from this private party, then the protections of the Fourth Amendment do not generally attach.

In practice, United States law affords some protections against public scrutiny of data collected by private parties. In many cases, the private party will refuse to give information to a law enforcement official without a subpoena or other formal order. Some companies perceive their business model to turn on whether they are trusted providers of Internet services, and as such make public their resistance to government demands, as Google successfully did against a Department of Justice request for a large amount of data on search queries; other firms, such as AOL, Yahoo!, and Microsoft, complied without a battle in court.[113]

What is different in an Internet era is that the vast majority of useful data about an individual is increasingly held in private hands—and individuals have a harder and harder time each year avoiding placing the data there in the first place. The emphasis in terms of legal protections on whether the observer is a public actor who carries out the search directly means that the core Constitutional protection is against "unreasonable searches."

2. The Perspective of the Observed

From the perspective of the person who is potentially observed—call her the "citizen"—"public" and "private" mean something different than what it means from the perspective of the person conducting the surveillance. What matters from the citizen's perspective is whether he or she has a reasonable expectation that the activities under surveillance are taking place in public or private.

There are three key problems that derive from this perspective in the digital age. The first is that the activity might be taking place in a context that the citizen believes is

---

[113] Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1; Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

"private," but where a third party is recording that activity. The recording might be taking place in a perfectly lawful, consensual way. For instance, the citizen signed up for an Internet Service Provider's package that permits access to the Internet, an email account, and a back-up service. Similarly, as researchers have shown, young people in particular consistently perceive their online audiences as more (and occasionally less) "private" than they really are.[114] For instance, they might post information to a page that they maintain on a social network site, such as MySpace or Facebook, to which only friends have access. In each of these cases, information might be shared in a certain context which feels "private" but which is plainly open to surveillance of multiple kinds. Neither the Fourth Amendment nor privacy-related statutes would protect the citizen, even if the citizen's perception of the context was "private."

Federal courts in the United States have addressed this general issue in several matters, but the law remains unsettled. In *Warshak v. United States*, the Sixth Circuit held that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP."[115] In a demonstration of how shaky the law is on this subject, the *Warshak* opinion was vacated on October 9, 2007, granting the government a rehearing en banc.[116] On rehearing, the constitutional question was avoided, as the court asserted that plaintiff's claim for injunction against future government action was not ripe.[117] Though the original *Warshak* opinion was vacated, the matter continues to be briefed

---

[114] danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics*
in Teenage Social Life, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA (David Buckingham ed., 2007), *available at* http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119 (last visited Nov. 28, 2008). Urs Gasser and I found much the same thing in our focus groups and interviews conducted while researching privacy matters for Born Digital.

[115] Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007); *see also* Katz v. United States, 389 U.S. 347, 351 (1967) (stating that something an individual "seeks to preserve as private" is therefore "constitutionally protected").

[116] *Warshak*, 490 F.3d at 455.

[117] Warshak v. United States, 532 F.3d 521 (6th Cir. 2008).

as of this writing, and scholars have already begun to take up the possible implications of such a ruling in depth.[118]

State courts have wrestled with this issue as well. In *State v. Reid*, the Supreme Court of New Jersey held that under a search and seizure provision of the New Jersey Constitution, a citizen has a protected privacy interest in information they provide to an ISP.[119] On the other hand, in *State v. Delp*, the Oregon Court of Appeals held that under Oregon law, the defendant did not have a privacy interest in non-content information disclosed to an ISP.[120]

The second, closely related problem is the difficulty, in a digital age, for the citizen to keep anything truly private from third parties. As the citizen's life is increasingly mediated by digital technologies, her social life, her work life, her civic life, and any other lives she leads are often led partly in digital public spaces. For those who carry BlackBerries on their hips or send text messages constantly, as many young people do, an increasing array of information about us is potentially in the hands of many people we do not know. In most cases, we also do not know what is being stored, for how long, and when and how it might be accessed or sold, by whom or to whom.

The final problem is that it is very difficult for the citizen to keep up with the pace of technological change. The rate of development of new digital technologies is very fast, such that even technology experts have little sense of what is even commercially available in fields tangentially related to their own. Few people would be knowledgeable enough about digital technologies to have an effective sense of what information they are sharing is publicly accessible and what is private.

This problem of keeping up with generally available digital technologies is particularly important in the context of the

---

[118] Tamar R. Gubins, *Warshak v. United States: The Katz for Electronic Communication*, 23 BERKELEY TECH. L. J. 723 (2008). *See also* ZITTRAIN, *supra* note 14, at 188; Orin Kerr, The Volokh Conspiracy, A Series of Posts on Warshak v. United States, *available at* http://volokh.com/posts/1182208168.shtml (last visited Oct. 22, 2008).

[119] State v. Reid, 945 A.2d 26, 33-34 (N.J. 2008).

[120] State v. Delp, 178 P.3d 259, 264 (Or. Ct. App. 2008).

Fourth Amendment. *Kyllo v. United States* holds an important place in the doctrine on Fourth Amendment law with respect to new technologies.[121] In *Kyllo*, the Court held that the use of technology to obtain any "information regarding the home's interior that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search—at least where (as here) the technology in question is not in general public use."[122] The last part of the *Kyllo* test is particularly important given the topic of this paper. The "general public use" test is vague and hard to implement. A search conducted with technologies that would seem to be in "general public use" may not be well known to a large percentage of a given population. Therefore, the use of new information technologies to conduct a search may not merit Fourth Amendment protection, even when the person being observed might expect the information to be protected.

B. Protecting What is "Reasonable"

The "reasonable expectation of privacy" standard is tricky even for law professors to understand. It is the most debated, puzzling aspect of Fourth Amendment jurisprudence, and scholarship.[123] For ordinary people, it is only getting more difficult—in a technological age—to develop a sense of what is reasonable. The range of possible surveillance methods at the network, server, and client levels underscore this difficulty facing citizens. Moreover, citizens face a dual bind: they need to decide whom to trust with their data (often private parties), but they also have to wonder—at the point of giving up control over their data—about who else might later access those data (often public entities).

As more and more of our lives are subject to these various forms of surveillance over "public" networks, it is crucial that some of our basic communications are treated as "private" under law. Some lower courts, in interpreting the Fourth Amendment,

---

[121] Kyllo v. United States, 533 U.S. 27 (2001).

[122] *Id.* at 28.

[123] Kerr, *Four Models of Fourth Amendment Protection*, *supra* note 16, at 504.

have suggested that sometimes actions in a public place, if meant to be private, might give rise to Constitutional protection. As one court held, "what a person knowingly exposes to the public through an open door or window does not receive Fourth Amendment protection, yet what a person tries to keep private, even in a public place, may be entitled to constitutional protection."[124] But the question of when data in public places online, if ever, give rise to such protections has not been made clear.

When it comes to the third-party data problem, though, there is little risk of misinterpreting the Supreme Court's current position. In 1976, the Court made plain that citizens have no reasonable expectation of privacy in data given by them to third parties in *United States v. Miller*.[125] Courts have long held that even evidence unlawfully obtained by a private party may later be used by a state actor against a defendant in a criminal proceeding.[126] The Fourth Amendment is usually implicated if a state actor *participates* in a search by a private party, or requests that a private party initiate the search, but that is not ordinarily the case in network, server, or client surveillance on the Internet.[127] Courts have held that a government search which occurs *after* a completed private search is lawful without a warrant if it does not exceed the scope of the private search.[128] The risk of government review of those data falls on the part of the person who deposited that information.[129]

In 1979, in *Smith v. Maryland*, the Court elaborated on the

---

[124] United States. v. Davis, 326 F.3d 361, 365 (2d Cir. 2003).

[125] 425 U.S. 435, 442-43 (1976).

[126] Burdeau v. McDowell, 256 U.S. 465, 476 (1921).

[127] *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(b) (4th ed. 2004) (detailing that the exclusionary rule applies to private searches or non-police searches where the government has requested the search, or has become involved with the search either at the beginning or at any time before the search is concluded).

[128] United States v. Jacobsen, 466 U.S. 109, 115 (1984) (noting that governmental actions pursuant to a private search of an individual's property or possessions "must be tested by the degree to which they exceed the scope of the private search").

[129] United States v. Miller, 425 U.S. 435, 443 (1976).

treatment of data given by an individual to a private third party.[130] The Court held that citizens have no reasonable expectation of privacy for the phone numbers they dial, because they voluntarily expose this information to their phone companies.[131] As a result, the Fourth Amendment protections did not attach in a case in which the government asked a phone company to install a pen register on a suspect's phone line.[132] This third-party doctrine becomes increasingly problematic as technology, and usage of it, evolves. While *Smith* may have had relatively narrow implications when originally decided, its holding might have much broader applicability in an Internet era since individuals knowingly give data to third parties when they send emails and other everyday digitally-mediated communications.[133] In spite of rapid technological change, *Smith* and *Miller* remain good law for the most part, though in some instances state courts have refused to define the Fourth Amendment privacy protections so narrowly, thus declining to follow the two cases on state law grounds.[134]

Much could have turned on the original holding in *Warshak*, if it were to become law. In the vacated *Warshak* opinion, the court noted a distinction between voluntarily submitting certain information to a third party, and exposing information to an "intermediary that merely has the ability to access the information sought by the government."[135] This distinction, if recognized by other courts, would conceivably disassociate the third-party doctrine developed in *Smith* and

---

[130] Smith v. Maryland, 442 U.S. 735 (1979).

[131] *Id.* at 742.

[132] *Id.* at 745-46.

[133] Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1338-39 (2002).

[134] *See, e.g.*, State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986) (holding that under the Washington Constitution, a citizen has a privacy interest in their phone records and thus a search warrant is necessary for the installation of a pen register); State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (holding that bank customers have a right of privacy in their bank records under the state constitution). *See also generally* Francis A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge for Traditional Legal Doctrine*, 24 RUTGERS COMPUTER & TECH. L.J. 305, 330 (1998).

[135] Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007).

Miller from Fourth Amendment issues regarding Internet usage. But absent a clear opinion of this sort, the third-party data issue continues to loom over commonplace activities by citizens over digital networks.

VI. TAKING UP THE "MOMENTOUS ISSUES"

Though technology may help safeguard personally identifiable information to some extent in a digital age, the answer is not likely that privacy can be enhanced through technology alone. The market can help, too, as firms compete to earn user trust, but it provides an imperfect solution at best. In addition, straight legal reform is unlikely to offer a complete answer. The amount of information about each person is growing and the ability to access it is likewise increasing. United States citizens are putting information about their lives into myriad public systems willingly.

Two proposals might help protect citizens in a digital era without unduly hampering the ability of law enforcement official to perform their job. First, courts might recognize circumstances in which citizens demonstrate an intent to keep data private when considering the extent to which those communications are deemed to be protected under law. Second, through legislation, states might extend a right to demand deletion to citizens to enable them to prompt the destruction after the fact of certain personally identifiable information held in private hands.

Courts might begin by recognizing a sliding scale that enables one to distinguish between those transactions, whether involved with public or private parties, that use digital networked technologies that give rise to some legal protection from government surveillance and those that do not. Imagine that a citizen sends an unencrypted email from her account with a commercial ISP, such as Verizon, to a friend, who uses Comcast as her ISP. The citizen believes that this email was "private." But plainly, in terms of both government and corporate ability to access it, that message is not "private." The email is recorded by her ISP; it is conveyed much as a postcard would be, across an open network; and it is recorded by her

friend's ISP. This communication is one in which the public actor would have little trouble gaining access and for which the law might offer, as today, little or no protection.

Especially if absent the protections that a *Warshak*-style holding might afford, a citizen ought to be able to manifest her intent to keep certain data communications private in a way the law might be able to recognize in various ways.[136] For instance, if that same email is encrypted from end-to-end, which is not technically difficult after setting up a basic system of communication, the message in every form—even when unencrypted, in plain text, and having traveled over public networks—might be deemed to have certain protections under law as "private" data. If that email was collected at a client on either end of the transaction, that data would receive additional protection under law. Likewise, an e-commerce transaction in which the citizen took steps to use a pseudonym or, more advanced, a zero-knowledge proof to identify herself only to a merchant (but not to someone intercepting the data) might be deemed to be "private"—as might the credit card information and other details of the transaction.[137] In other words, if a citizen expresses her intent for a certain transaction to be

---

[136] It is of course the case that there are certain statutory protections for personal data under United States law, such as the 1974 Privacy Act (5 U.S.C. § 552a). In particular, the Privacy Act requires that federal agencies use personal data only for its intended purpose. *See* 5 U.S.C. §§ 552a(e)(1), (3)(B) (2008). In practice, however, the effect of this statute in terms of citizen protection has been modest. There are additional statutory limitations to sharing information between private parties and the government. For a specific example, see the 1986 Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11, under the Electronic Communications and Privacy Act ("ECPA"), which provides limitations to the sharing of information between an electronic communications service and a law enforcement agency. Under the SCA, a provider may only voluntarily disclose the contents of a communication to a law enforcement agency where (1) the service provider inadvertently obtained the information and (2) the information appears to pertain to criminal activity. 18 U.S.C. § 2702(b)(7)(A)(i)-(ii) (2008). Alternatively, a governmental entity may *require* that a provider disclose certain electronic communication information, but in most instances a warrant is necessary. *See* 18 U.S.C. § 2703 (2008). The European Commission has similarly struggled with these issues, and has sought to place strong, comprehensive protections for citizens.

[137] *See* Anna Lysyanskaya, *Cryptography: How to Keep Your Secrets Safe*, SCI. AM., Sept. 2008, *available at* http://www.sciam.com/article.cfm?id=cryptography-how-to-keep-your-secrets-safe (last visited Nov. 28, 2008).

private, using either proprietary or widely accessible technical means, the law could meet her partway. The obvious shortcomings of this intent-based approach include the subjective nature of intent generally and the extent to which an encrypted email (one related to which the intent has been manifested) is less likely to be subject to surveillance by the very nature of its protection.

Second, the law might also be amended to help a citizen demand that information about him or her held by private firms be taken out of the "public" space after the fact. Since one of the fears about government surveillance is the ability to search in oceans of data, held in private hands after the fact, a citizen might be permitted by law to demand that her account not only be closed, but all data associated with her name be deleted by the technology service provider.[138] Such a "right to demand deletion" would have demerits, to be sure.[139] The costs

---

[138] *See* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2005), *available at* http://www.harvardlawreview.org/forum/issues/119/dec05/ohm.pdf, responding to Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) (for discussion of such a right that might be embedded in Fourth Amendment protections). *See also* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2 (2008).

[139] Paul Schwartz alludes to an idea similar to the right to demand deletion in his discussion of privacy-control in the internet age. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000). Schwartz notes that in light of rising privacy concerns due to rapid technological change, there is agreement that privacy means individuals should have the right to control the use of the data they disperse over the internet. *Id.* at 820. This is what he terms the "privacy-control" paradigm. *Id.* However, Schwartz ultimately rejects the privacy-control paradigm, noting that given collective action problems, bounded rationality, and informational asymmetries, informational self-determination is not a realistic goal. *Id.* at 822. He additionally notes that given public accountability and bureaucratic rationality considerations, it is not clear that privacy concerns trump other needs requiring that this information not be secluded from the public realm. *Id.* at 828. Though Schwartz critiques privacy-control, the alternative he proposes still assigns value to the idea that individuals should have some control over the information they disperse on the internet, but that this right is not absolute. *Id.* at 834. Thus Schwartz champions constitutive privacy, claiming that "information privacy norms should create shifting, multidimensional data preserves that insulate personal data from different kinds of observation by different parties. Different kinds of 'outing,' that is, revelation of otherwise fully or partially hidden aspects of one's life, should be prevented before different audiences." *Id.* at 834-35.

Lior Jacob Strahilevitz discusses generally a "right to destroy," but he does not discuss it in the context of the Fourth Amendment or privacy rights. Lior Jacob

associated with implementing such a system would be high for the private sector; law enforcement officials would inevitably lose access to potentially very useful information about criminals who invoke the law to protect evidence of their wrongdoing; and some companies might be prompted to aggregate more personal information with someone's identity in order to be able to comply with deletion orders. Any legislative fix of this sort would need to be drafted carefully to mitigate these potential harms.[140]

Other legislative steps might make sense over time, especially to the extent that the third-party data problem grows as reliance on digitally mediated technologies, using private services, grows.[141] A further legislative rule might be enacted to stop certain government means of accessing personally identifiable data held in private hands, such as the purchase of data from data brokers. Likewise, rules might limit the uses to which such aggregated data are put by government actors, such as limits on sharing data across agencies for purposes other than that for which the data was initially collected. A tort-based regime might help to regulate the sharing or disclosure of information across the public-private border to the extent that rigorous procedures are not honored during the transfer.[142] And

---

Strahilevitz, *The Right to Destroy*, 114 YALE L.J. 781 (2005). Rather, Strahilevitz refers to the right to destroy as a property right—one of the "sticks in the bundle of [property] rights." *Id.* at 794. Ohm and Strahilevitz accept a right to destroy/delete as pre-existing, and the conclusion follows that if such a right is a defined property interest, then the Fourth Amendment is implicated when the government interferes with an individual's right to delete.

[140] There is a closely analogous right to disclosure and correction included in the EU privacy rights and in U.S. safe harbor definition related to the EU Privacy Directive.

[141] Fred Cate, for instance, proposes a selection of statutory protections to fill the gap in privacy protections affected by the *Smith* and *Miller* decisions in the internet age. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008). Cate proposes (among other things) the authorization of data mining programs that promote accountability, oversight, and compliance with legal requirements. *Id.* at 487. He suggests that such programs should be strictly limited, both in terms of who can use data mining systems, and in terms of the quantity and quality of information revealed. *Id.*

[142] One critique of the current law/tort-regime is that there is usually no suppression remedy in this sort of legal action. Though the ECPA may regulate government access to electronic communication information collected by a third party, Fourth Amendment

still others have argued that the problems of informational privacy in a digital age are best solved through the courts.[143]

The market, too, might help citizens, though the limits of a purely market-based solution are quickly evident. Some firms do compete on the basis of establishing "best practices" for protecting consumer data; Google signaled their leadership on privacy in resisting the Department of Justice's demand for search data. In the international context, a series of technology companies is working on a code of conduct to govern when they will turn data over to state actors.[144] Best practices for businesses and easy-to-understand icons for citizens might provide a greater sense to citizens of the risks that they run by using certain services. These icons might make clear, for instance, how long data collected by a certain firm are retained and how the company responds to government requests for information. But citizens would need to be savvy enough to interpret the relevant market signals. And the core third-party data problem—the government's ability to access these data held in "public" places—would be little changed. If we leave it to the market alone, no meaningful legal barrier would be erected between the private sector players and the public agencies.

---

remedies are not available for victims of an ECPA violation. Though government entities are liable to suit under the ECPA, it has been held that the statute does not afford a suppression remedy. *See* Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996); *see also* United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000).

[143] Ric Simmons, for instance, asserts that in *Katz*, the court delineated a results-based test rather than a method-based rule for decision in Fourth Amendment cases. Simmons, *supra* note 133. According to Simmons, the Katz court intended that Fourth Amendment protections attach to particular kinds of information collected, as opposed to particular search methods used. *Id.* In decisions like *Smith*, courts have strayed from the *Katz* results-based test and adopted more of a methods-based test. If the court returns to a results-based test, it is plausible to expect that Fourth Amendment protections attach to information dispersed over the Internet that an individual has intended to keep private.

[144] *See* http://cyber.law.harvard.edu/research/principles; *see also* Jonathan Zittrain & John Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 103-22 (Ronald Deibert, John Palfrey, Rafal Rohizinski, & Jonathan Zittrain eds., 2008).

VII. Conclusion

Ultimately, we as citizens need to decide how much access to the increasingly rich records of our lives we want to grant our law enforcement officials. At present, in practice, we as citizens would need to limit what we turn over to private parties if we wish to limit what the state can come to know about us. As the court said in *Garcia*, "Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues. . . ."[145] These momentous issues play out at the United States border with cyberspace, and at international borders, many times every day.

Given what we know about how people are leading their lives mediated by digital technologies, and given what we know about how much surveillance can happen in converged public and private spaces online, it is time that we take up these issues directly and re-evaluate the inevitable trade-offs we are making every day. Central to the challenge that we face is an information asymmetry: while we have an all-too-graphic idea of the high costs of not ensuring our security today, we know too little about what others will be able to come to know about us in the future. What we do know is that the third-party data problem grows with each passing year. We know that private entities collect much data about us. We know that the law affords citizens little protection from abuse by either public or private parties. And we know that the rules that we set today to govern the collection, sharing, and access of data will have long-term consequences, both for security and for individual privacy. Based upon these facts, it is time to rethink whether the scope of the Fourth Amendment is sufficient to protect individual privacy from intrusion by the state, especially with respect to data initially collected by private parties. More fundamentally, it is also time to consider whether the public-private distinction, as it has developed over the past century and a half, makes sense in a digital age.

---

[145] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

BORDER SEARCHES IN THE AGE OF TERRORISM

*Robert M. Bloom**

INTRODUCTION

The debate between individual freedom and the power of the executive—a contest hotly disputed throughout our nation's history—rages during times of national crisis. The terrorist attacks of September 11, 2001, represent a crisis of unprecedented magnitude. Reflecting on the likely effects of 9/11 on the legal world, Supreme Court Justice Sandra Day O'Connor captured this sentiment in a speech at New York University Law School mere weeks after that infamous day:

> The trauma that our nation suffered will [alter] and has already altered our way of life, . . . and it will cause us to reexamine some of our laws pertaining to criminal surveillance, wiretapping, immigration, and so on . . . . As a result, we are likely to experience more restrictions on our personal freedom than has ever been the case in our country.[1]

Justice O'Connor's words are likely prophetic when considering the effect that terrorism and national security concerns will have on Fourth Amendment jurisprudence. This article will focus on an area where terrorism and national

---

* Professor of Law, Boston College Law School. I wish to thank Beth Hanrahan, a student in the class of 2010 at Boston College Law School, for her valuable assistance.

[1] JEFFREY TOOBIN, THE NINE: INSIDE THE SECRET WORLD OF THE SUPREME COURT 206-07 (2007) (quoting a speech given by Justice O'Connor at New York University Law School on September 28, 2001).

security concerns are at their highest: border searches.

Despite any early, post-9/11 fears, such as those voiced by Justice O'Connor—that the judiciary would adopt its traditional posture of deference to the executive in times of national crisis[2]—the Supreme Court has in fact shown an unexpected willingness to review and restrict the power of the executive,[3] at least when faced with due process concerns. We refer to the string of cases concerning the status of those captured and detained by the United States during its "War on Terror," cases in which the Court has, time and again, acted not in deference to the executive but out of fealty to one of "freedom's first principles":[4] individual rights.

The group of cases decided on June 28, 2004, *Rasul v. Bush*,[5] *Hamdi v. Rumsfeld*[6] and *Rumseld v. Padilla*,[7] were viewed by many as a harbinger of change.[8] In *Rasul*, the petitioners, twelve Kuwaitis and two Australians captured abroad and being held in military custody at the United States Naval Base at Guantanamo Bay, Cuba, brought suit in federal court in Washington, D.C., challenging the legality of their detention.[9] The government defended on procedural grounds,

---

[2] *See* David Rudovsky, *The Impact of the War on Drugs on Procedural Fairness and Racial Equality*, 1994 U. CHI. LEGAL F. 237, 238-39 (1994). Rudovsky notes:

> Historically, wars (both hot and cold) have placed great stress on constitutional rights, and these pressures have led the courts to countenance substantial limitations on liberty. The internment of Japanese-Americans during World War II, the suspension of the writ of habeas corpus during the Civil War, the imprisonment of strikers and dissidents during World War I, and the McCarthy tactics of the Cold War were all justified in the name of war. During each of these periods, the Supreme Court gave virtually complete deference to inflated Executive claims of imminent danger to the country.

Id. (footnotes omitted).

[3] *See* Steven R. Shapiro, *The Role of the Courts in the War Against Terrorism: A Preliminary Assessment*, 29 FLETCHER F. WORLD AFF. 103, 103 (2005).

[4] *See* Boumediene v. Bush, 128 S. Ct. 2229, 2277 (2008).

[5] 542 U.S. 466 (2004).

[6] 542 U.S. 507 (2004).

[7] 542 U.S. 426 (2004).

[8] *See* Shapiro, *supra* note 3, at 103 ("Whether process and transparency will be enough to preserve civil liberties in an age of terrorism remains to be seen. It is, nonetheless, more than the courts have often demanded in the past during other periods of national crisis. For that reason alone, it is an encouraging sign.").

[9] *Rasul*, 542 U.S. at 470-71.

arguing that U.S. courts lacked jurisdiction to hear the case.[10] The Supreme Court decided in favor of the petitioners, holding that the federal habeas statute confers on the district courts jurisdiction to hear petitioners' habeas corpus challenges.[11]

The legality of an American citizen's detention as an enemy combatant at a naval brig in Charleston, South Carolina, was at issue in *Hamdi*, where the Court held that, although Congress authorized the detention of combatants in the narrow circumstances alleged in this case, due process demands that a citizen held in the United States as an enemy combatant be given a meaningful opportunity to contest the factual basis for that detention before a neutral decision maker.[12] The Court faced similar questions in *Padilla*, although it never reached the merits of the case, dismissing instead on procedural grounds.[13]

In 2006, in *Hamdan v. Rumsfeld*,[14] the Court again found in favor of the petitioner, a Yemeni national captured in Afghanistan and held at Guantanamo Bay.[15] In its decision, the Court held that the military commissions established by the President to try Guantanamo Bay detainees were not expressly authorized by any congressional act and that the military commission procedures violated the Uniform Code of Military Justice and did not satisfy the Geneva Conventions.[16] In the wake of the *Hamdan* decision, Congress enacted the Military Commissions Act of 2006,[17] which specifically authorized the use of military commissions to try unlawful enemy combatants.[18]

---

[10] *Id.* at 475.

[11] *Id.* at 485.

[12] Hamdi v. Rumsfeld, 542 U.S. 507, 508-39.

[13] Rumsfeld v. Padilla, 542 U.S. 426, 430 (holding Padilla's petition had been improperly filed in New York instead of South Carolina where he was being detained, the Court stated, "We confront two questions: First, did Padilla properly file his habeas petition in the Southern District of New York; and second, did the President possess authority to detain Padilla militarily. We answer the threshold question in the negative and thus do not reach the second question presented.").

[14] 548 U.S. 557 (2006).

[15] *Id.* at 566-67.

[16] *Id.*

[17] Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2600 (codified at 10 U.S.C. §§ 948-50 (2006)).

[18] This congressional action cleared the way for Hamdan's war crimes trial by

This congressional action was the subject of *Boumediene v. Bush*[19] in 2008. At issue was Section Seven of the Act which denied the federal courts jurisdiction to hear habeas actions such as the case at bar.[20] The Court held, in part, that the petitioners—aliens designated as enemy combatants and held at Guantanamo Bay—were entitled to the habeas privilege.[21] The Court held that Section Seven operated as an unconstitutional suspension of the writ because the government had not implemented an adequate and effective substitute review process, as required by the writ's Suspension Clause.[22] In other words, these Guantanamo Bay detainees had the constitutional right to challenge their detention in U.S. federal courts.[23]

These decisions have been hailed as the Supreme Court's "harsh rebuke" of the Bush Administration and its efforts to curtail individual rights in the name of national security. These decisions have, some might say, tipped the scale in favor of

---

military commission, which commenced on July 21, 2008. His attempt to delay the trial, in light of the Supreme Court's decision in *Boumediene v. Bush*, was unsuccessful. The *Boumediene* decision was held to apply only to those detainees not yet facing any war crimes or criminal charges. Thus *Boumediene* has not prevented the trial by military commission of those detainees already facing charges, such as Hamdan, from moving forward. On August 6, 2008, a U.S. military jury found Hamdan guilty of providing material support for terrorism. His attorneys will likely appeal. *See* William Glaberson, *Panel Convicts bin Laden Driver in Split Verdict*, N.Y. TIMES, August 7, 2008, at A1; *see also* Scott Shane & William Glaberson, *Rulings Clear Military Trial of a Detainee*, N.Y. TIMES, July 18, 2008, at A1; Jerry Markon, *Detainee's Trial in Military System Begins Today*, WASHINGTON POST, July 21, 2008, at A03; *see infra* note 23 and accompanying text (for a brief discussion of the *Boumediene* decision and its impact on the Guantanamo Bay detainee cases generally).

[19] 128 S. Ct. 2229 (2008).

[20] *Id.* at 2242.

[21] *Id.* at 2262.

[22] *Id.* at 2274.

[23] *Id.* at 2277. The *Boumediene* decision opened the door for the more than 270 detainees held at Guantanamo Bay to challenge their detention. *See* Robert Barnes, *Justices Say Detainees Can Seek Release*, WASHINGTON POST, June 13, 2008, at A01 (summarizing the *Boumediene* decision and providing a brief history of the Guantanamo Bay detainee cases). Those challenges have begun to move forward, with District Court Judge Thomas F. Hogan, who is overseeing a majority of the cases, urging expediency on all sides. *See* Matt Apuzzo, *Judge to White House: Guantanamo is Top Priority*, ASSOCIATED PRESS, July 8, 2008.

personal liberties.[24] However, these decisions reflect the Court's inclination toward a preservation of *due process* rights alone. All of the plaintiffs were already in custody and seeking a hearing to challenge their detention. The Fourth Amendment, on the other hand, goes to the issue of what the government can do to *investigate* terrorism. Specifically, Fourth Amendment jurisprudence, with reasonableness as its touchstone,[25] allows the Court to weigh or balance concerns of terrorism and national security as part of its decision-making process.[26] In this way, the Fourth Amendment provides the mechanism for considering terrorism concerns. Thus, the question of reasonableness—which balances the government interest (which surely includes the great destruction to life and property caused by terrorism) against the level of privacy intrusion on the individual—lends itself to Justice O'Connor's prediction more readily than do questions of due process. Our focus will be how terrorism and national security concerns affect Fourth Amendment determinations generally, as well as specifically in the border search area.

---

[24] *See, e.g.*, David Stout, *Justices Rule Terror Suspects Can Appeal in Civilian Courts*, N.Y. TIMES, June 13, 2008, *available at* http://www.nytimes.com/2008/06/13/washington/12cnd-gitmo.html.

[25] *See* United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))); *see also* Pennsylvania v. Mimms, 434 U.S. 106, 108-09 (1977); Terry v. Ohio, 392 U.S. 1, 19 (1968).

[26] The Fourth Amendment is made up of two clauses joined by the conjunction "and": "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. The first clause speaks to being secure against unreasonable searches and seizures, and the second clause lays out the requirements for warrants including probable cause and specificity. For much of the history of the Fourth Amendment, in order to give meaning to the vague term "unreasonable," the Court read the two clauses together. So a search, to be reasonable, would require a warrant with justification and specificity, otherwise it would be per se unreasonable. However, for the last thirty years, the Court has opted to analyze reasonableness on its own—warrants and justification, therefore, are but a factor in determining reasonableness. The balancing test is reflective of this approach.

This article will first explore the history of border searches. It will look to the reorganization of the border enforcement apparatus resulting from 9/11 as well as the intersection of the Fourth Amendment and border searches generally. Then, it will analyze the Supreme Court's last statement on border searches in the *Flores-Montano*[27] decision, including what impact this decision has had on the lower courts. Finally, the article will focus on Fourth Amendment cases involving terrorism concerns after 9/11, as a means of drawing some conclusions about the effect the emerging emphasis on terrorism and national security concerns will likely have on border searches in this post-9/11 world.

I. HISTORY

A. Legislative

The government has restructured its border operation since 9/11. The United States Border Patrol (USBP), founded in 1924, has had many responsibilities during its history. It has often reflected changing societal concerns. As a result of 9/11 and the ensuing Homeland Security Act of 2002,[28] the USBP was moved from the dissolved Immigration and Naturalization Service to within the Department of Homeland Security (DHS). In this way, the Border Patrol and the inspection division of the Immigration and Naturalization Service were for the first time brought under a single umbrella: the newly-created Department of Homeland Security. USBP is now a segment of Customs and Border Protection under the directorate of Border and Transportation Security, which reports directly to the director of Homeland Security. Part of the primary mission of the DHS is to "prevent terrorist attacks within the United States" and "reduce the vulnerability of the United States to terrorism."[29] In recent testimony before the Senate Finance Committee, Ronald

---

[27] 541 U.S. 149 (2004).

[28] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

[29] 6 U.S.C. § 111 (2004).

Colburn, Deputy Chief of the U.S. Border Patrol, said "our main function is to prevent the illegal entry of terrorists, criminals, illegal aliens, illegal narcotics, contraband as well as smugglers who operate between ports of entry."[30] It is interesting to note that the first topic he mentioned was terrorists.

Greater cooperation between agencies has also resulted since 9/11. The Terrorist Screening Center (TSC) has been established so that the federal government can better process terrorist informants. The FBI and the DHS created watch lists of informants with the TSC acting as a central repository of such information. The TSC and the Terrorists Screening Database (TSDB) are administered by the FBI and include all individuals believed to have any degree of terrorism nexus. The TSDB included more than 200,000 names with each person being assigned a category of terrorist threat.[31]

After being consolidated within the DHS, the border agencies, which were renamed the U.S. Bureau of Customs and Border Protection, continued to be responsible for enforcing U.S. immigration laws, administering U.S. customs laws, and "securing the borders."[32] They were also given a new principal responsibility: "Preventing the entry of terrorists and the instruments of terrorism into the United States."[33] During the last decade manpower has nearly tripled. The number of border patrol agents has grown from approximately 5,900 in 1996 to approximately 18,000 today.[34] It should be pointed out that not only has there been greater scrutiny at the border, but there has been a tightening of the requirements to obtain a visa.[35] This

---

[30] *Border Security Before the S. Comm. on Finance*, 2007 WL 2802236 (statement of Ronald Colburn, Deputy Chief, U.S. Border Patrol).

[31] *See* Rahman v. Chertoff, 244 F.R.D. 443, 446 (N.D. Ill. 2007).

[32] 6 U.S.C. § 542 (2002) (codifying the Reorganization Plan Modification for the Department of Homeland Security, H. Doc. 108-32 (2003)).

[33] 6 U.S.C. § 202(1) (2002).

[34] GAO, *Border Patrol: Costs and Challenges Related to Training New Agents: Hearing Before the Subcomm. on Mgmt., Investigations, & Oversight of the H. Comm. on Homeland Sec.*, GAO-07-997T (2007) (statement of Richard M. Stana, Dir., Homeland Sec. & Justice Issues).

[35] *See* James Glanz, *Study Warns of Lack of Scientists as Visa Applications Drop*, N.Y. TIMES, Nov. 20, 2003, at A28.

increase in personnel and restructuring demonstrates the heightened scrutiny at the border in light of the "War on Terror."

B. Courts

As early as 1886, the Supreme Court pointed out the importance of border searches.[36] The court in *Boyd v. United States* indicated that Congress had passed a statute[37] authorizing the seizure[38] of non-customed goods two months before it passed the Fourth Amendment. "[C]ustoms officials [had] 'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed.'"[39] Therefore, it was evident the drafters of the Constitution did not believe searches and seizures at the border were unreasonable.[40] This was reiterated in 1925 in *Carroll v. United States*.[41] This case involved the smuggling of alcohol during prohibition. The Court, in dicta, indicated that the rationale for the *per se* reasonableness of searches and seizures at the border went beyond merely collection of duty but was also derived from concerns of national security. The Court noted that "travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[42]

Thus there is recognition that the nation can control whom and what may enter the country.[43] From its historical roots of preventing the entry of uncustomed goods, search and seizure at the border has extended to protection from the entry of

---

[36] *See* Boyd v. United States, 116 U.S. 616 (1886).

[37] Act of July 31, 1789, 1 Cong. ch. 5, § 24, 1 Stat. 29, 43.

[38] United States v. Ramsey, 431 U.S. 606, 616 (1977).

[39] *Id.* (quoting Act of July 31, 1789, 1 Cong. ch. 5. § 24, 1 Stat. 29, 43).

[40] *See Boyd*, 116 U.S. at 623.

[41] 267 U.S. 132, 147-50 (1925).

[42] *Id.* at 154.

[43] *See Ramsey*, 431 U.S. at 620.

undesirable people, drug interdiction, preventing the import of dangerous material, and, since 9/11, to working on preventing terrorists and instruments of terrorism from crossing the border.[44]

Moreover, there has been a long-standing recognition that border searches are *per se* reasonable. Historically, border searches have been allowed without the two primary protections of the Fourth Amendment: probable cause and the need for a warrant. Border search represents one of the original exceptions to the Fourth Amendment warrant requirement. Attempts to utilize the border search exception at places other than the border have not been successful.[45]

As time has passed, border searches have merged into the evolving administrative or regulatory search doctrine. These searches have one common element: they are not being done for the normal law enforcement goal of finding criminals but for goals unrelated to criminal investigation. The Fourth Amendment approach to these searches was introduced in *Camara v. Municipal Court*.[46] In this case involving inspections for housing code violations, the Court acknowledged that the traditional requirement of probable cause and resulting warrant for Fourth Amendment activity would not work; there was no individualized suspicion because health inspection would usually involve large areas of concern, not individual houses. As such, the Court turned to the reasonableness clause of the

---

[44] *See, e.g.*, United States v. Brignoni-Ponce, 422 U.S. 873 (1975); Almeida-Sanchez v. United States, 413 U.S. 266 (1973).

[45] These searches at locations other than the border have required some justification. *See, e.g.*, *Brignoni-Ponce*, 422 U.S. at 884 ("Except at the border and its functional equivalents, officers on roving patrol may stop vehicles only if they are aware of specific articulable facts, together with rational inferences from those facts, that reasonably warrant suspicion that the vehicles contain aliens who may be illegally in the country."); *Almeida-Sanchez*, 413 U.S. at 272-73 ("Whatever the permissible scope of intrusiveness of a routine border search might be, searches of this kind may in certain circumstances take place not only at the border itself, but at its functional equivalents as well. . . . But the search of the petitioner's automobile by a roving patrol, on a California road that lies at all points at least 20 miles north of the Mexican border, was of a wholly different sort. In the absence of probable cause or consent, that search violated the petitioner's Fourth Amendment right to be free of unreasonable searches and seizures.").

[46] 387 U.S. 523 (1967).

Fourth Amendment and devised a balancing test. The Court balanced the need to search—the government interest—with the scope of the intrusion resulting from the search, saying that "there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."[47] In the health inspection search, so as to limit the discretion of the inspector which might result in a greater intrusion, a standardized approach involving neutral criteria was required. Thus, on one hand, the Court considers the degree to which the seizure or search intrudes upon an individual's privacy, and, on the other hand, it considers the degree to which the seizure or search promotes the government interest. In analyzing reasonableness, the Court looks to "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[48] Reasonableness of searches has become the touchstone of Fourth Amendment analysis.[49]

Border searches coupled with terrorism concerns also bring to mind a category of administrative searches sometimes referred to as "special needs" searches. Justice Blackmun, who coined the phrase in a high school search case, described special needs as those "beyond the normal need for law enforcement, mak[ing] the warrant and probable cause requirement impracticable."[50] He found the school setting to represent exceptional circumstances. Also included in this category of special needs are the search of a government employee's office for professional misconduct,[51] the search of a probationer's home,[52] or the suspicionless search of probationers.[53]

As we will see, border searches have fallen comfortably

---

[47] *Id.* at 536-37.

[48] Illinois v. Lidster, 540 U.S. 419, 427 (2004) (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)).

[49] *See, e.g.*, Maryland v. Wilson, 519 U.S. 408, 411 (1997).

[50] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

[51] *See* O'Connor v. Ortega, 480 U.S. 709 (1987).

[52] *See* Griffin v. Wisconsin, 483 U.S. 868 (1987).

[53] *See* Samson v. California, 547 U.S. 843 (2006).

within this balancing framework. The important government interest side of balancing with regard to reasonableness has been the basis of border searches, as the Court indicated in *United States v. Ramsey*.[54] "[S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[55] On the intrusion side of the balance, since everyone is subject to such searches (the old adage "misery loves company"), there is less of an intrusion.[56] Thus ordinary or routine searches at the border can be made without a warrant or individual suspicion. In determining what is ordinary or routine, one must consider the objective of the border search: the vital national interest to protect against persons and things coming into our country. Given this interest, then, intrusions, including searches of outer clothing, luggage, shoes, pockets, contents of mail, wallets, and purses, are routine and require no justification.[57] When the scope of the intrusion increases to the extent that the border search is no longer routine, then some justification might be required.

This increasing justification reasoning is reminiscent of the approach in *Terry v. Ohio*[58] and elaborated on in *United States v. Sharpe*.[59] *Terry*, a case involving the so-called stop-and-frisk

---

[54] 431 U.S. 606, 616 (1977).

[55] *Id.*

[56] *See* Delaware v. Prouse, 440 U.S. 648, 664 (1979) (Rehnquist, J., dissenting). Justice Rehnquist in dissent opined:

> Because motorists, apparently like sheep, are much less likely to be "frightened" or "annoyed" when stopped en masse, a highway patrolman needs neither probable cause nor articulable suspicion to stop *all* motorists on a particular thoroughfare, but he cannot without articulable suspicion stop *less* than all motorists. The Court thus elevates the adage "misery loves company"to a novel role in Fourth Amendment jurisprudence.

Id.

[57] *See* United States v. Thirty-Seven Photographs, 402 U.S. 363 (1971) (seizure of photographs); United States v. Tsai, 282 F.3d 690 (9th Cir. 2002) (search of luggage and briefcase); United States v. Grayson, 597 F.2d 1225 (9th Cir. 1979) (examination of papers found in pockets); Henderson v. United States, 390 F.2d 805 (9th Cir. 1967) (search of purse).

[58] 392 U.S. 1 (1968).

[59] 470 U.S. 675 (1985).

doctrine, allowed for a search based upon less justification than probable cause because the intrusion was less than a full-scale arrest.[60] As the intrusion increases so too must the justification. In *Terry*, to determine whether the search was unreasonable, the Court devised a two-step analysis. First, the Court asked, was the Fourth Amendment activity justified at its inception?[61] Next, the Court found it necessary to analyze the scope of the search: the government's conduct "must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[62] To state it differently, the Court will take into account the purpose of the stop and the time and manner needed to effectuate that purpose. In considering the scope, the Court must examine whether law enforcement officers diligently pursued their purpose:

> In assessing whether a detention is too long in duration to be justified as an investigative stop, we consider it appropriate to examine whether the police diligently pursued a means of investigation that was likely to confirm or dispel their suspicions quickly, during which time it was necessary to detain the defendant.[63]

Again, as the justification increases, so can the scope of the search. The scope includes both the manner and length of detention.[64]

In *Illinois v. Caballes*,[65] for example, the respondent was stopped for speeding on an interstate highway.[66] As the first trooper on the scene was writing a warning ticket, a second trooper arrived with his drug-detection dog.[67] The dog signaled the presence of drugs in the trunk of the respondent's car, and

---

[60] 392 U.S. at 25-26.

[61] *Id.* at 20.

[62] *Id.* at 19 (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)).

[63] *Sharpe*, 470 U.S. at 686.

[64] *See* Muehler v. Mena, 544 U.S. 93, 98-100 (2005); United States v. Brignoni-Ponce, 422 U.S. 873, 881-82 (1975).

[65] 543 U.S. 405 (2005).

[66] *Id.* at 406.

[67] *Id.*

the officers searched the contents of the trunk, found marijuana, and immediately arrested the respondent.[68] The question on which the Supreme Court granted certiorari was "[w]hether the Fourth Amendment requires reasonable, articulable suspicion to justify using a drug-detection dog to sniff a vehicle during a legitimate traffic stop."[69] Although the Court recognized that a "seizure that is justified solely by the interest in issuing a warning ticket to the driver can become unlawful if it is prolonged beyond the time reasonably required to complete that mission," [70] the facts did not support such a finding in *Caballes*. The duration of the stop, the Court concluded, was "entirely justified by the traffic offense and the ordinary inquiries incident to such a stop."[71] It should be pointed out that the dog was readily available and additional time was not necessary to secure the presence of the dog.[72] In the Court's view, conducting a dog sniff would not change the character of the stop unless the sniff itself infringed upon the respondent's constitutionally protected interest in privacy.[73] Since there is no Fourth Amendment reasonable expectation of privacy in a dog sniff, the Court found no such constitutionally protected privacy interest here,[74] and therefore the sniff was not a search subject to the Fourth Amendment.[75]

---

[68] *Id.*

[69] *Id.* at 407.

[70] *Id.*

[71] *Id.* at 408.

[72] *See id.*

[73] *Id.*

[74] *Id.* ("We have held that any interest in possessing contraband cannot be deemed 'legitimate,' and thus, governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'").

[75] *Id.* at 408 ("Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." (quoting United States v. Jacobsen, 466 U.S. 109, 123 (1984))); *see also* Muehler v. Mena, 544 U.S. 93, 101 (2005) (holding, in part, that there was no additional seizure within the meaning of the Fourth Amendment, and thus no further justification required for officers' questioning of respondent about her immigration status while executing a search warrant, because respondent's initial detention was lawful and her lawful detention was not prolonged by the questioning).

United States v. Montoya de Hernandez[76] provides a useful framework for a *Terry* analysis in the border area. In this case, a woman entering the country from Bogota, Columbia, was suspected of being a so-called "balloon swallower."[77] She was held for almost sixteen hours before customs officials sought a court order for an x-ray, pregnancy test, and rectal examination, as she refused to use the toilet. During this period, she had not defecated, urinated, or had food or drink.[78] Ultimately, she was taken to a hospital where a physician removed a foreign substance from her rectum.[79] "[O]ver the next four days[, the woman] passed 88 balloons containing a total of 528 grams of 80 percent pure cocaine hydrochloride."[80] To determine the Fourth Amendment reasonableness of the intrusion, the Court balanced the intrusion with the legitimate governmental interest.

In looking at the government interest, the court recognized the government's broad power to conduct border searches to protect the nation by stopping and examining persons coming into the country.[81] "At the border, customs officials have more than merely an investigative law enforcement role. They are also charged, along with immigration officials, with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives."[82] This power is "qualitatively different at the international border than in the interior."[83] Because of this, the balance favors the government at the border. In this case, the Court highlighted the border concerns by pointing out the "veritable national crisis in law enforcement caused by smuggling of illicit narcotics."[84]

On the intrusion side of the equation, the Court evaluated

---

[76] 473 U.S. 531 (1985).

[77] *Id.* at 534 (explaining that a balloon swallower is one who hides drugs in their alimentary canal).

[78] *Id.* at 535.

[79] *Id.*

[80] *Id.* at 536.

[81] *Id.* at 538.

[82] *Id.* at 544.

[83] *Id.* at 538.

[84] *Id.*

the sixteen-hour detention and the ultimate examination of the rectum. The court of appeals evaluating the intrusion questioned the "humanity" of holding someone "until her bowels moved, knowing that she would suffer 'many hours of humiliating discomfort.'"[85] The Supreme Court, although finding the "intrusion beyond [a] routine" border search, opted for a lesser "reasonable suspicion" standard as opposed to a higher "clear indication" standard.[86] Finding that the government did have a "particularized and objective basis" [87] to meet the reasonable suspicion standard, the Court turned to the scope to ask if it was reasonably related to the justification. The Court expressed reluctance to get into an after-the-fact evaluation, and stated that the mere fact that there were less intrusive ways to accomplish the objective would not necessarily render the search unreasonable.[88] The Court rejected any time limits and instead opted for a common sense approach to evaluate the intrusion.[89]

Justice Brennan in dissent, upset about the length of detention and methods used in this case, thought that the justification should have been presented to a judicial officer, otherwise a great deal of authority is allocated to low-ranking officials. He argued:

> Something has gone fundamentally awry in our constitutional jurisprudence when a neutral and detached magistrate's authorization is required before the authorities may inspect 'the plumbing, heating, ventilation, gas, and electrical systems' in a person's home, investigate the back rooms of his workplace, or poke through the charred remains of his gutted garage, but *not* before they may hold him in indefinite involuntary isolation at the Nation's border to investigate whether he might be engaged in criminal wrongdoing. No less than those who conduct administrative searches, those charged with investigative duties at the border "should not be the sole

---

[85] *Id.* at 536.

[86] *Id.* at 541.

[87] *Id.* at 541-42 (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

[88] *Id.* at 542.

[89] *See id.* at 543.

> judges of when to utilize constitutionally sensitive means in pursuing their tasks," because "unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy."[90]

Searches of persons such as that which occurred in *Montoya de Hernandez* are regarded as non-routine.[91] These searches require justification—usually reasonable suspicion. It should be pointed out that reasonable suspicion was all that was required in the very intrusive search in *Montoya de Hernandez*. So a border search which falls under the rubric of "routine" requires no further justification other than the fact that it occurs at the border. However, when the search involves greater intrusion, it is classified as "non-routine," and some additional level of justification is required.[92]

The last case involving border searches decided by the

---

[90] *Id.* at 555-56 (Brennan, J., dissenting) (footnote omitted) (quoting United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 317 (1972)).

[91] *See id.* at 541-42 (majority opinion); *see also* United States v. Guadalupe-Garza, 421 F.2d 876, 878 (9th Cir. 1970)).

[92] The routine versus non-routine distinction usually focuses on the physical aspects of the search, such as disrobing, exposing intimate body parts, forced intrusions causing pain, and physical contact. *See, e.g.*, United States v. Braks, 842 F.2d 509 (1st Cir. 1988); *see also* Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 997-98 (2007).

In *Bradley v. United States*, the search included a pat down of Bradley's dress by a female inspector who then used her fingers to push on Bradley's breasts and inner and outer labia. 299 F.3d 197, 201 (3d Cir. 2002). This pat down was regarded as routine even though it included patting of the clothing outside sensitive areas. *Id.* at 204. Non-routine searches were regarded as strip searches, body cavity searches and pat downs that involved fondling or penetration. *Id.* at 205.

The category of routine border searches includes: pat down searches for weapons or contraband, the removal of shoes and outer garments, the emptying of pockets, purses and wallets, the use of drug sniffing dogs, the cutting of a spare tire, and x-ray searches of inanimate objects. *See* United States v. Cortez-Rocha, 383 F.3d 1093, 1100-01 (9th Cir. 2004) (cutting of spare tire); United States v. Kelly, 302 F.3d 291, 294-95 (5th Cir. 2002) (canine sniff); United States v. Beras, 183 F.3d 22, 24 (1st Cir. 1999) (pat down of defendant); United States v. Sandler, 644 F.2d 1163, 1169 (5th Cir. 1981) (pat down of defendant).

X-ray searches have been considered no more intrusive than a strip search and a more dignified alternative to a body-cavity search. *See* United States v. Vega-Barvo, 729 F.2d 1341, 1348 (11th Cir. 1984).

Supreme Court was *United States v. Flores-Montano*.[93] In *Flores-Montano*, the Court was faced with the question of whether the dismantling and search of a full gas tank needed additional justification.[94] After an initial inspection of a car, it was sent to a secondary inspection station.[95] A customs inspector tapped the gas tank and, when it sounded solid, requested a mechanic to remove the tank.[96] A mechanic arrived within twenty to thirty minutes and then spent between fifteen and twenty-five minutes disconnecting the gas tank from the car.[97] The inspector hammered off Bondo (a putty-like substance used to seal openings) and found thirty-seven kilograms of marijuana blocks.[98]

The Ninth Circuit relied on the *Montoya de Hernandez* routine/non-routine distinction in its analysis of the search, finding that such searches were non-routine and therefore required reasonable suspicion.[99] The court of appeals also relied on *United States v. Molina-Tarazon*,[100] one of its previous decisions. It is interesting to note the reasoning of the court in *Molina-Tarazon* as it specifically dealt with the search of inanimate objects as opposed to a body search. In determining that the search of the gas tank was non-routine, the court looked at three contributing factors: the force used to remove and disassemble the gas tank, the risk of harm involved in the procedure, and the diminished sense of security experienced by the individual whose vehicle was searched in such a manner.[101]

When *Flores-Montano* was before the Supreme Court, the government chose not to argue the need for any justification to disassemble and search the gas tank even though there was

---

[93] 541 U.S. 149 (2004).

[94] *See id.* at 150.

[95] *Id.*

[96] *Id.* at 151.

[97] *Id.*

[98] *Id.*

[99] *See id.* at 150-52.

[100] 279 F.3d 709 (9th Cir. 2002).

[101] *Id.* at 713-14.

some justification (the tank "sounded solid").[102] In this way, the government deliberately raised the issue of what constitutes routine or non-routine. Keep in mind, a non-routine search would require some justification. However, the Supreme Court rejected the lower court's use of the *Montoya de Hernandez* routine/non-routine distinction when dealing with a search of property as opposed to an individual. The Court, in distinguishing privacy concerns of persons from those of property and, in particular, automobiles, said that "complex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles."[103] In this way, the Court seemed to discount the necessity of determining when a non-bodily search, such as an automobile search, would ever be characterized as non-routine; thus the routine/non-routine distinction appears inapplicable to property border searches. The Court said "[i]t is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment."[104] In responding to the danger issue raised in *Molina-Tarazon*, the Court pointed out that gas tank searches could be conducted without damaging the vehicle, the process was easily reversible, and there was no evidence of any accidents resulting from disassembly.[105] Since the facts did not raise the issue of drilling or other permanent destruction of the vehicle, the court refused to consider it.[106] Even though a motorist's interest is "not insignificant" when the government removes, disassembles and reassembles a gas tank, it is outweighed by "the Government's interest of preventing the entry of unwanted persons and effects[, which] is at its zenith at the . . . border."[107] Persons crossing the border have a reduced

---

[102] *Flores-Montano*, 541 U.S. at 151.

[103] *Id.* at 152.

[104] *Id.* at 154.

[105] *Id.* at 154-56.

[106] *See id.*

[107] *Id.* at 152.

expectation of privacy.[108] Balancing the strong governmental interests and lesser privacy expectations, most searches at the border fall within a routine category. The Court has left a narrow opening if the process would have destroyed the property.[109] Within this possible exception, it appears as though the Court would only consider non-routine searches as those involving body searches, as demonstrated by the facts of *Montoya de Hernandez*, which included an intrusive body cavity search and x-ray examination, as well as a time of detention of over sixteen hours.

A question unresolved by *Flores-Montano* involves whether laptop computers should be regarded as property similar to an automobile. Laptop computers store a great deal of personal effects, including e-mails, photos, and financial material, often spanning many years:

> While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound.[110]

Such capabilities bring to mind the sentiment expressed by the dissenting opinion in *Olmstead v. United States*[111] by Justice Brandeis, recognizing the importance of one's innermost thoughts:

> The makers of our Constitution . . . recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts,

---

[108] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

[109] *Flores-Montano*, 541 U.S. at 154-56.

[110] United States v. Arnold, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008).

[111] 277 U.S. 438 (1928).

> their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[112]

Nevertheless in cases after *Flores-Montano*, circuits have treated the computer as property not requiring any additional justification for searches. For example, the Fourth Circuit in *United States v. Ickes*,[113] recognizing the government's broad authority to conduct border searches, refused to carve out a First Amendment exception for computers at the border.[114] In expressing concern for protecting the sovereign from terrorists, the court stated: "Particularly in today's world, national security interests may require uncovering terrorist communications, which are inherently 'expressive.'"[115] The court was also reluctant to create a standard which would distract customs officials from "policing our borders and protecting our country."[116]

Additionally, the Ninth Circuit in *Arnold*,[117] overturning a lower court decision, interpreted *Flores-Montano* as not distinguishing automobiles from other property. According to the court, because the computer was property, it did not implicate the same concerns as the search of a person.[118] The

---

[112] *Id.* at 478 (Brandeis, J., dissenting).

[113] 393 F.3d 501 (4th Cir. 2005).

[114] *Id.* at 506.

[115] *Id.* Ickes argued that *Ramsey* was willing to afford greater protection to expressive material. The Fourth Circuit pointed out that *Ramsey* did not draw such a line. *Ramsey* found it "unnecessary to consider the constitutional reach of the First Amendment in this area in the absence of existing statutory and regulatory protection" *Id.* at 507 (quoting United States v. Ramsey, 431 U.S. 620, 624 (1977)).

[116] *Id.* at 506.

[117] 523 F.3d 941 (9th Cir. 2008).

[118] *See id.* at 945-46; *see also* United States v. McAuley, 563 F. Supp. 2d 672, 677 (W.D. Tex. 2008) ("The Defendant would like the Court to believe that the search of his computer was unauthorized because he maintains a higher degree of privacy in his computer, due to the personal nature of information contained therein. The Defendant claims that any search of a computer is akin to a bodily search of a person and should be categorized as a non-routine search requiring a finding of reasonable suspicion in order to conduct such a search. The Defendant would have this Court impute the same level of privacy and dignity afforded to the sovereignty of a person's being to an inanimate object like a computer. The Court finds this argument without merit. Relying on the Supreme

court further cited *Flores-Montano* for the proposition that the distinction between routine and non-routine was simply inapplicable when dealing with property.[119] In this decision, there was no analysis of the intrusiveness of computer searches. U.S. Customs and Border Protection has elaborated on the search of computers, allowing for the taking, retaining, copying, and sharing of the information on these computers. These computers may be retained for a reasonable time.[120] The policy emphasizes that all this may be done without any individualized suspicion.[121]

In *United States v. Ramsey*,[122] a case involving a border search of an envelope, Justice Rehnquist indicated that a search of the envelope for contraband was different than reading correspondence in the envelope.[123] Arguably, to actually read the correspondence would violate the Fourth Amendment.[124] The Ninth Circuit's reading of *Flores-Montano* puts this idea into question, as any search of property at the border would now seem to be justified without the need for further justification. It bears mentioning that, given the huge intrusion resulting from computer searches, one would think that the balance would tip so as to require some level of justification. This proposition has

---

Court's reasoning in *Flores-Montano*, this Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents.").

[119] *See id.* at 945; *see also* United States v. Lawson, 461 F.3d 697, 700 (6th Cir. 2006) ("An x-ray examination of a *person*, it is true, may require some level of suspicion . . . because it may permit greater intrusions into the privacy and dignity of the individual [, b]ut 'the same is not true about x-rays of objects.'") (quoting United States v. Okafor, 285 F.3d 842, 845 (9th Cir. 2002)) (citations omitted); United States v. Hernandez, 424 F.3d 1056, 1057 n.2 (9th Cir. 2005) ("As we explain, this routine/non-routine analytical framework has been denounced by the Supreme Court insofar as searches of property are concerned."); United States v. Camacho, 368 F.3d 1182, 1185 (9th Cir. 2004) ("The Supreme Court has now disapproved *Molina-Tarazon*.").

[120] U.S. CUSTOMS AND BORDER PROTECTION, POLICY REGARDING BORDER SEARCH OF INFORMATION (July 16, 2008), http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.

[121] *Id.*

[122] 431 U.S. 606 (1977).

[123] *Id.* at 623-24, 624 n.18.

[124] *See id.* at 624.

been supported by some lower courts which have indicated that it is one thing to allow for a perusal of a document to verify that it contains no contraband but another thing entirely to read a document, such as a diary, which could deal with very personal matters.[125]

Lower courts have expanded on what is appropriate under *Ramsey*. In *United States v. Seljan*,[126] border inspectors as part of a currency interdiction program opened a FedEx box and discovered a letter. They quickly scanned the letter and saw indication of pedophilic activity. The defendant argued that to actually read the letter required some justification. The court found scanning (reading a few words) to be reasonable even without justification. Raising the issue of terrorism, the court said that there should not be "unreasonable constraints" on custom officials examining documents, as such constraints could result in overlooking detection plans for explosive devices, instructions for an attack, chemical formulas for poison, or other types of information related to terrorism.[127] In the en banc decision, Chief Judge Kozinski in his dissent points out that the founders had great concern for protecting "the privacy of thoughts and ideas." This is clearly indicated by the inclusion of the term "papers" in the actual text of the Fourth Amendment. Kozinski further points out that giving custom officials free reign to search unless they destroy property or invade the body

---

[125] *See, e.g.*, United States v. Soto-Teran, 44 F. Supp. 2d 185, 191 (E.D.N.Y. 1996). For photocopying or closely reading documents, usually reasonable suspicion is required. *See* United States v. Schoor, 597 F.2d 1303, 1306 (9th Cir. 1979); *Soto-Teran*, 44 F. Supp. 2d at 191.

[126] 497 F.3d 1035 (9th Cir. 2007), *aff'd en banc* No. 05-50236, 2008 U.S. App. LEXIS 22056 (Oct. 23, 2008).

[127] United States v. Seljan, 2008 U.S. App. Lexis 22056, at *29 n.9 (9th Cir. 2008) (en banc). In the en banc decision, Judge Callahan concurrence stated, "'[p]articularly in today's world, national security interests may require uncovering terrorist communications, which are inherently expressive.'" *Id.* at *48 (Callahan, J. concurring) (quoting United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005)). Judge Callahan concurring also points out that Congress pursuant to 19 U.S.C. § 1583 restricts custom inspectors from searching international mail weighing sixteen ounces or less sent via the U.S. Postal Service. A person could therefore avoid the reading of the contents of her correspondence if she sent it via U.S. Postal Service as opposed to Federal Express. *Id.* at *55-56.

is simply too much leeway.[128] Despite Kozinki's eloquence, the Ninth Circuit's reading of *Flores-Montano* would seem to allow for the reading of a laptop's contents without further justification.[129]

It should be reiterated that the only exception with regard to property searches mentioned in *Flores-Montano* was the possibility that some inanimate object searches would become non-routine when they involved the destruction of property. Destruction of property and the reusability of the car appeared to be important factors. The Court in *Flores-Montano* commented in a footnote that they had no reason to consider drilling, as the case involved removal, disassembly, and reassembly.[130] In a Ninth Circuit case after *Flores*, the situation involved the cutting open of a spare tire. The court found that this was not unreasonably destructive, as the vehicle could still be operated safely.[131]

II. TERRORISM AND THE BORDER

In the government briefs for *Flores-Montano*, the issue of terrorism was raised. The United States pointed out that gas tanks could not only be used to smuggle narcotics but also be used as instruments of terror.[132] To emphasize this point, the Government referenced the case of Ahmed Ressam, a would-be terrorist who had explosives hidden in the trunk of his vehicle which were to be detonated at Los Angeles International Airport.[133] The Government argued that if a trunk can be searched without reasonable suspicion but a gas tank cannot be,

---

[128] *Id.* at *57-72 (Kozinski, C.J., dissenting).

[129] These cases raise many concerns especially when considering laptop searches at the border. Apparently, the Department of Homeland Security is routinely searching laptops as American reenter the United States from abroad. With the discretion allotted to border patrol agents, it is not surprising that selective ethnic groups could be targeted for more extensive searches. *See* Austin Bogues, *Laptop Searches in Airports Draw Fire at Senate Hearing*, N.Y. TIMES, June 26, 2008, at A17.

[130] United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004).

[131] *See* United States v. Cortez-Rocha, 383 F.3d 1093, 1096 (9th Cir. 2004).

[132] Brief for the United States at 18, United States v. Flores-Montano, 541 U.S. 149 (2004) (No. 02-1794), 2003 WL 22873083.

[133] United States v. Ressam, 221 F. Supp. 2d 1252 (W.D. Wash. 2002).

it will encourage terrorists to hide materials in the gas tank.[134] A brief by the Washington Legal Foundation, a public interest law center with its objective of promoting national security, also strongly argued for suspicionless searches as an important means to prevent terrorist attacks. Thus, the Court was certainly made aware of the terrorist threat.[135]

In overturning *United States v. Molina-Tarazon*,[136] which required reasonable suspicion for a fuel tank search, the Court may have been considering the terrorist threats when it said "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[137] The concern over terrorists at the border can also be found in the circuits. The Third Circuit states: "[I]t is beyond peradventure, as the Seventh Circuit has noted, that 'the events of September 11, 2001, only emphasize the heightened need to conduct searches' at our borders."[138]

Terrorism objectives fall comfortably into the category of cases involving so-called "special needs" searches.[139] The Government made an unsuccessful argument of special needs in *City of Indianapolis v. Edmond*.[140] In *Edmond*, a traffic checkpoint program, using roadblocks, designed to interdict illegal narcotics was held to violate the Fourth Amendment because its primary purpose was to detect crime.[141] However, once it is established that there are needs beyond normal law enforcement, balancing to determine reasonableness kicks in. In conducting this balance, courts consider the government interest, including the weight and immediacy of the government objective, as well as whether the search will accomplish this

---

[134] Brief for the United States, *supra* note 132, at 18.

[135] *See* Brief of Wash. Legal Found. & Allied Educ. Found. as Amici Curiae Supporting Petitioner, United States v. Flores-Montano, 541 U.S. 149 (2004) (No. 02-1794), 2003 WL 22873084.

[136] 279 F.3d 709 (9th Cir. 2002).

[137] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

[138] United States v. Bradley, 299 F.3d 197, 202 (3d Cir. 2002) (quoting United States v. Yang, 286 F.3d 940, 944 n.1 (7th Cir. 2002)).

[139] *See supra* notes 50-53 and accompanying text.

[140] 531 U.S. 32, 48 (2000).

[141] *Id.*

objective. The nature and character of the intrusion is weighted against this government interest. It is interesting to note that the *Edmond* court in dicta indicated that a roadblock could be employed without a warrant or reasonable suspicion to "thwart an imminent terrorist attack."[142]

A case involving a search in the New York subway to address terrorism concerns presents a useful illustration of this balancing, as well as a special needs search. [143] The court indicated that terrorism was indeed a special need.[144] Moreover, the court felt it was not necessary to demonstrate any specific impending threat and instead talked about the objective of preventing a pervasive threat from spreading.[145] Further, in light of the fact that there were thwarted plots in the New York subway as well as recent bombings in Madrid, London, and Moscow, the threat was imminent and the risk high. Although the court recognized the Fourth Amendment protects an individual's right in the contents of packages brought into subways, it felt the intrusion was not great: passengers received notice of the search and could decline the search as long as they left the subway, and the search was limited only to containers that could contain explosives and to only a visual inspection unless it was necessary to manipulate.[146] Further, the officers would not read printed or written material or request any personal bodily inspection.[147] The search itself only lasted a matter of seconds, and there was no danger of the arbitrary use of power and no discretion exercised by the police because they stopped everyone.[148] With regard to the effectiveness of the search, the court gave great deference to law enforcement officials who had "'a unique understanding of, and responsibility

---

[142] *Id.* at 44.

[143] *See* MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006).

[144] *See id.* at 263.

[145] *See id.* at 272. *See also* Board of Education v. Earls, 536 U.S. 822 (2002) (employing the same approach and speaking of a general threat resulting from a pervasive drug problem among our nation's youth as sufficient immediacy).

[146] *MacWade*, 460 F.3d at 273.

[147] *Id.*

[148] *Id.*

for, limited public resources, including a finite number of police officers.'"[149] Therefore, the court did not inquire greatly into the effectiveness, instead opting to determine if it was reasonably effective to accomplish the government objective of deterring and detecting a terrorist attack on the subway system.[150] The fact that searches were done at random subway stations did not alter its effectiveness because expert testimony indicated that terrorists want predictable and vulnerable targets and the random nature of the program generated uncertainty, which deters attacks.[151]

The case of *Tabbaa v. Chertoff*[152] deals squarely with issues of terrorism at the border and probably describes the present state of Fourth Amendment doctrine at the border. The case was a civil action in which the plaintiffs claimed, among other things, that their Fourth Amendment rights were violated by the border patrol.[153] Based on intelligence, the U.S. Bureau of Customs and Border Patrol planned an inspection operation to carefully screen individuals who attended the Reviving the Islamic Spirit (RIS) Conference at the Sky Dome in Toronto, Canada.[154] It should be noted that an estimated 13,000 people from across North America attended the RIS Conference.[155] The intelligence indicated that persons with terrorist ties as well as known terrorists would be attending the conference.[156] Everyone who attended, upon their re-crossing the border, was subject to a screening procedure which permitted border officials

---

[149] *Id.* (quoting Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 454 (1990)).

[150] *Id.* at 273-75.

[151] It should be pointed out that even though the justification for these searches is to protect our national security against the threat of terrorism and not to obtain evidence to use in criminal prosecutions, the evidence resulting from such searches is often used in ordinary (non-terrorist) criminal prosecutions. *See* Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 193 (2006).

[152] 509 F.3d 89 (2d Cir. 2007).

[153] *Id.* at 91.

[154] *Id.* at 93-94.

[155] *Id.* at 94.

[156] *Id.* at 93.

to fingerprint and photograph them.[157] Plaintiffs, who had attended the conference for religious reasons, had no criminal records and there was no evidence they had committed a crime or were associated with terrorists.[158] Nevertheless, plaintiffs, after they had affirmatively indicated they had been to the conference, were ordered to pull their cars into a separate area and enter a nearby building.[159] While their cars were searched, the plaintiffs were frisked, questioned, fingerprinted, and photographed. Each of the plaintiffs was "detained and searched for between four and six hours."[160] The frisk involved CBP officers forcefully kicking the plaintiffs' feet open and almost knocking them to the ground in order to effectuate the search.[161] Plaintiffs were not, however, subject to strip, body cavity or involuntary x-ray searches.[162]

The issue before the court in *Tabaa* was whether the detention and search was so invasive as to be beyond a routine border search. The Second Circuit was asked to determine the precise line between what is routine and what is not routine.[163] The court has held that "[r]outine searches include those searches of outer clothing, luggage, a purse, wallet, pockets, or shoes which, unlike strip searches, do not substantially infringe

---

[157] *Id.* at 93-94.

> In response to this intelligence information, CBP prepared an Intelligence Driven Special Operation ("IDSO"). An IDSO is a directive to particular ports of entry to undertake special enforcement actions to meet specific concerns raised by intelligence information. Under the IDSO in this case, the Buffalo port of entry, among others, was instructed to identify and examine persons associated with the RIS conference or other similar conferences taking place in Toronto who sought entry to the United States. The Buffalo port was directed to contact the National Targeting Center ("NTC") of CBP if persons identified in the IDSO were encountered in order to determine whether the individuals posed a particular threat.

Tabbaa v. Chertoff, No. 05-CV-582S, 2005 WL 3531828, at *3 (W.D.N.Y. Dec. 22, 2005) (citations omitted).

[158] *Tabbaa*, 509 F.3d at 94.

[159] *Id.*

[160] *Id.* at 95.

[161] *Id.*

[162] *Id.* at 98-99.

[163] *See generally* Unites States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006).

on a traveler's privacy rights."[164] More invasive searches, like "strip, body cavity, or involuntary x-ray searches" are not routine and require reasonable suspicion level of justification.[165] The spectrum between a full body cavity search and the time of detention in *Montoya de Hernandez* and quick searches at the border of clothing and luggage usually accomplished in a short time is great. The question the court faced in this case was: Where does this terrorist-style processing fall within the spectrum?

Plaintiffs argued the search was not routine.[166] First, plaintiffs alleged that being selected for intrusive questioning, photographing and fingerprinting in a separate building with other Muslims created a stigma, whereas searches of cars or luggage to which everyone is subject does not create such a stigma.[167] They further argued that CBP threatened to detain them until they cooperated, and finally argued that a time of detention of four to six hours should not be considered routine.[168] The court analyzed each aspect of the procedure taken by the CBP and concluded that none of the factors were non-routine.[169] Even the kicking of the feet was not as invasive as lifting a shirt.

The court did, however, recognize that the cumulative effect of several routine searches could reach the level of non-routine, but did not find such a cumulative effect in this case.[170] Stigmatization did not reach the level of a body cavity or strip

---

[164] *Id.* (citing United States v. Grotke, 702 F.2d 49, 51-52 (2d Cir. 1983)).

[165] United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985).

[166] *Tabbaa*, 509 F.3d at 97-101.

[167] *Id.* at 98-99.

[168] *Id.* at 99-101.

[169] *Id.* at 101. *See* United States v. Silva, 715 F.2d 43, 47 (2d Cir. 1983) (noting that questions about citizenship, the length and purpose of an applicant's trip to Canada, and what items she had acquired or bought in Canada are all routine). Likewise, pat-down searches have repeatedly been found to be routine, even when they were followed by the lifting of an applicant's shirt or forced removal of shoes. *See, e.g.*, United States v. Charleus, 871 F.2d 265, 268 (2d Cir. 1989) (noting "the light touching of appellant's back followed by a lifting of his shirt arguably straddles the line between the two categories of border searches," and can be considered a routine search because the "potential indignity . . . failed to compare with the much greater level of intrusion associated with a body or full strip search.").

[170] *Tabbaa*, 509 F.3d at 99.

search or involuntary X-ray as in *Montoya de Hernandez*. "Because the decisive factor in the analysis is invasiveness of privacy—not overall inconvenience . . . searches of plaintiffs, considered in their entirety, were routine in the border context, albeit near the outer limits of what is permissible absent reasonable suspicion."[171]

With regard to the threatening behavior, the court cited *Ramsey* for the proposition that threatening extended detention for failing to comply with screening measures is "an important aspect of the 'longstanding right of the sovereign to protect itself' at the border, and therefore is 'reasonable simply by virtue of the fact that [it] occur[s] at the border.'"[172] "In other words, border crossers cannot, by their own non-compliance, turn an otherwise routine search into a non-routine [search]."[173]

The four to six hour time of detention falls somewhere between the sixteen hours in *Montoya de Hernandez* and the one-hour delay in *Flores-Montano*.[174] The court asked itself whether the detention was reasonably related to the justification for it.[175] Although the court recognized the inconvenience of the four to six hour detention, it suggested that such a time-frame, by itself, would not render the search non-routine especially in the border context.[176]

CONCLUSION

Congress has shown a willingness to defer to the executive branch. After *Hamdan* indicated that a specific Congressional enactment was required,[177] Congress acted accordingly. The

---

[171] *Id.*

[172] *See id.* at 100 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1972) (alterations in original)).

[173] *See id.*

[174] *See* United States v. Flores-Montano, 541 U.S. 149, 155 n.3 (2004) ("Respondent points to no cases indicating the Fourth Amendment shields entrants from inconvenience or delay at the international border.").

[175] *See Tabbaa,* 509 F.3d at 100 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 542 (1985)); s*ee also* United States v. Sharpe, 470 U.S. 675, 682-85 (1985).

[176] *See Tabbaa*, 509 F.3d at 100-01.

[177] *See supra* notes 14-18 and accompanying text.

Court overturned the act, in part, in *Boumediene*.[178] Recently Congress has once again shown deference to the executive branch by allowing for expansion of its surveillance power, including immunity for phone companies that cooperated with the National Security Agency.[179] The Court appears to be the only branch of government that will review the executive power in accordance with the checks and balances envisioned by our founding ancestors. One is reminded of Justice O'Connor's words in *Hamdi*, in which she warned that "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens."[180]

Will the reasonableness clause of the Fourth Amendment take into account terrorism concerns? [181] The Supreme Court has only specifically addressed the Fourth Amendment and its relation to national security issues such as terrorism in 1972. In *United States v. United States District Court (Keith)*,[182] the Court sought to address executive branch surveillance in a national security context. In *Keith*, electronic wiretaps were used against U.S. citizens who were suspected of conspiracy to bomb U.S. government property.[183] These wiretaps were authorized by the U.S. Attorney General but without any court authorization.[184] Justice Powell for the unanimous Court balanced the government interest to protect national security against the invasion on individual privacy.[185] While the Court was prepared to accept some different Fourth Amendment rules in this context, it emphasized that some Fourth Amendment

---

[178] Boumediene v. Bush, 128 S. Ct. 2229 (2008). *See supra* note 18 and accompanying text.

[179] *See* Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1.

[180] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2006).

[181] *See* John T. Parry, *Terrorism and the New Criminal Process*, 15 WM. & MARY BILL RTS. J. 765, 810-11 (2006) ("[F]or reasonableness to work in the interpretation of the right that limits police authority to search and seize, courts must put a thumb on the government's side of the scale when they craft doctrine.").

[182] 407 U.S. 297 (1972).

[183] *Id.* at 299-300.

[184] *Id.* at 299.

[185] *Id.* at 314-21.

safeguards were still necessary (e.g., warrants).[186]

Is there a greater acceptance by the Court of police power since 9/11? To the extent that the Court has discussed this, it has indicated a greater sensitivity to police methods. In *United States v. Drayton*,[187] the Court pointed out greater cooperation in the age of terrorism between citizens and the police: "[B]us passengers answer officers' questions and otherwise cooperate not because of coercion but because the passengers know that their participation enhances their own safety and the safety of those around them."[188] As previously mentioned, *City of Indianapolis v. Edmonds*,[189] a case involving a traffic checkpoint program designed to interdict illegal narcotics, was held to violate the Fourth Amendment because its primary purpose was to detect crime. Nonetheless, the Court in dicta mused that a suspicionless roadblock would be permissible if employed to "thwart an imminent terrorist attack."[190]

This article has analyzed the likely outcomes of the law and the flexibility with which the Fourth Amendment can be manipulated to accomplish the objectives of limiting individual rights at the border. The reasonableness approach to the Fourth Amendment, with its balancing analysis, supplies the method for the Court to consider terrorism. Justice Brennan, dissenting in *New Jersey v. T.L.O.*,[191] described this balancing as "Rohrschach-like" and characterized the Court's reasoning as "preordained."[192] With the flexibility inherent in such balancing, one is reminded of the words of Justice Felix Frankfurter: "It is true also of journeys in the law that the place you reach depends

---

[186] For a comprehensive discussion of *Keith*, the executive's use of warrantless NSA surveillance and the Fourth Amendment, see Bloom & Dunn, *supra* note 151. In response to *Keith* and President Nixon's abuse of power during the Watergate scandal, Congress conducted an extensive inquiry into the activities of the nation's intelligence agencies (the Church Committee hearings). The result of these hearings was the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. *See id.* at 155-56.

[187] 536 U.S. 194 (2002).

[188] *Id.* at 205.

[189] 531 U.S. 32 (2000).

[190] *Id.* at 44.

[191] 469 U.S. 325 (1985) (Brennan, J., dissenting).

[192] *Id.* at 358.

on the direction you are taking. And so, where one comes out on a case depends on where one goes in."[193]

To the extent that the American public has been polled since 9/11, there is generally support for greater security measures even if these measures infringe on individual privacy.[194] Will the reasonable balancing allowed by the Fourth Amendment provide for the insinuation of popular sentiment into court decisions? The courts have always provided a safeguard for constitutional protection. The protection remains regardless of public outcry. The Constitution was designed to protect law abiders and law breakers. The words of Chief Justice Tauro of the Massachusetts Supreme Judicial Court, in declaring that the death penalty was unconstitutional under the Massachusetts Constitution, come to mind:

> [J]udges cannot look to public opinion polls or election results for constitutional meaning as has been suggested. It is our duty to interpret the Constitution to the best of our personal abilities and judgment. Our constitution requires that we be 'as free, impartial and independent as the lot of humanity will admit.' If we succumb to contemporary public opinion we lose that requisite independence and impartiality demanded of us and fail totally in our purpose.[195]

Terrorism has changed the landscape. Given the enormous dangers to life and property from terrorist acts, it has increased the government's interest exponentially.[196] In analyzing terrorism, we are forced to make accommodations. As Justice Scalia wrote in *Anderson v. Creighton*, "regardless of the terminology used, the precise content of most of the Constitution's civil-liberties guarantees rests upon an assessment of what accommodation between governmental need and individual freedom is reasonable."[197] This is also true in our

---

[193] United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).

[194] *See* Robert C. Power, *Changing Expectations of Privacy and the Fourth Amendment*, 16 WIDENER L.J. 43, 44 (2006).

[195] Commonwealth v. O'Neal, 339 N.E.2d 676, 692 (Mass. 1975) (quoting MASSACHUSETTS DECLARATION OF RIGHTS, art. 29).

[196] *See* MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006).

[197] 483 U.S. 635, 643-44 (1987).

Fourth Amendment analysis of reasonableness.

Nevertheless, I am reminded of Justice Potter Stewart's words. Justice Stewart, in 1971, referencing the Fourth Amendment, observed:

> [T]his basic law and the values that it represents may appear unrealistic or 'extravagant' to some. But the values were those of the authors of our fundamental constitutional concepts. In times not altogether unlike our own they won . . . a right of personal security against arbitrary intrusions by official power. If times have changed, . . . the changes have made the values served by the Fourth Amendment more, not less, important.[198]

The balancing of individual rights with security concerns was addressed by Israel's Chief Justice of the Supreme Court Aharon Barak in 2004, when he ordered the removal of a portion of the West Bank Security Wall due to its burden on the Palestinians:

> We are aware that in the short term, this judgment will not make the state's struggle against those rising up against it any easier . . . This is the destiny of a democracy: she does not see all means as acceptable, and the ways of her enemies are not always open before her. A democracy must sometimes fight with one arm tied behind her back. Even so, democracy has the upper hand. The rule of law and individual liberties constitute an important aspect of her security stance.[199]

If the war on terrorism is fought in a way that ignores our democratic ideals, we have lost the war.

---

[198] Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) (footnote omitted).

[199] Gareth Evans, President, Int'l Crisis Group, 2005 Wallace Wurth Lecture at the University of New South Wales, Sydney: The Global Response to Terrorism 10 (Sept. 27, 2005) (alteration in original) (transcript available at http://www.unsw.edu.au/news/pad/articles/2005/sep/FINALWurthLectureTerrorismGE.pdf); *see also* Michael S. Greco, President's Message, *A False Choice: The American People Should Not Be Forced to Choose Between Freedom and Security*, A.B.A. J., April 2006, at 6, 6 ("The [P]resident has a sacred obligation under the Constitution to protect both the nation's safety and its constitutionally-guaranteed freedoms–and to honor the doctrine of separation of powers. His failure to do so would compromise the very principles and ideals that we are fighting to protect.").

ESSAY

ELECTRONIC SURVEILLANCE AT THE VIRTUAL BORDER

*Susan Freiwald**

Before the advent of globalization, physical borders between countries played the crucial role in differentiating legal systems. Travelers from one country to another usually knew that they were also moving out of one system of laws into another. In most cases, they either encountered physical landmarks, or they had to get past border officials who controlled passage. A nation-state made its own laws that it imposed on the people within its border, including, of course, those who had crossed into its territory. Borders separated those subject to both the burdens and privileges of a nation's laws from those subject to neither. In short, borders distinguished the area in which a particular sovereignty was exercised from the areas in which it was not.

As Professors Johnson and Post observed in an influential essay in the Stanford Law Review, cyberspace has fundamentally challenged the efficacy of traditional physical borders.[1] Internet users can easily "visit" web sites established in a foreign country without that country's government being

* Professor, University of San Francisco School of Law. I thank Peter Volz for his excellent research assistance and Gretchen Harris and the other editors of the Mississippi Law Journal. I also thank Patricia L. Bellia, Leah Freiwald, Gus Guibert, and Peter Jan Honigsberg for their helpful comments. Any errors are mine.

[1] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

aware of their "arrival." The dramatic increase in electronic movements across borders, whether as communications or transactions, has meant that the traditional physical means of policing borders no longer work as effectively.[2] Johnson and Post argued that the "borderlessness" of cyberspace calls into question both the efficacy and legitimacy of "territorial sovereign" regulation of cyberspace.[3] They argued that cyberspace citizens should play a greater role than traditional sovereigns in setting the legal rules to govern cyberspace.[4] Their proposal garnered substantial academic response, with some vocal critics proclaiming that traditional legal rules based on territorial sovereignty still functioned well, notwithstanding the move into the electronic sphere.[5]

Johnson and Post published their essay on cyberspace borders in 1996, in the early days of the World Wide Web. Since then, lawmakers have drafted numerous laws designed specifically to address new problems arising in cyberspace.[6] Here in the United States, for example, Congress has designed new rules to handle intellectual property infringement based in cyberspace,[7] and has tried several times to regulate indecency online, only to have its statutes overturned by the Supreme Court's application of the First Amendment to cyberspace.[8]

---

[2] *Id.* at 1372; *see also* LAWRENCE LESSIG, CODE VERSION: 2.0, 10-11 (2006) (discussing borderlessness of cyberspace and its implications).

[3] Johnson & Post, *supra* note 1, at 1370-76.

[4] *See id.* at 1374.

[5] *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); *see also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 485-89 (2000) (arguing that self-governance is inconsistent with liberal ideas).

[6] *See generally, e.g.*, PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE (3d ed. 2007).

[7] Digital Millennium Copyright Act ("DMCA"), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.); *see also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 1991) (describing the DMCA as something "Congress enacted in 1998 to strengthen copyright protection in the digital age").

[8] *See, e.g.*, Ashcroft v. ACLU, 542 U.S. 656, 674 (2004) (rejecting a statutory attempt to "regulate the vast content of the World Wide Web at its source" as too costly to "First Amendment values"); Reno v. ACLU, 521 U.S. 844, 870 (1997) (noting that "our cases provide no basis for qualifying the level of First Amendment scrutiny that should be

Meanwhile, courts have interpreted pre-cyber statutes in new cyberspace contexts and have extended common law precedents into cyberspace settings.[9] It therefore seems right to assume, at this point, the legitimacy of a sovereign's imposition of its own legal rules on the cybercitizens within its physical territory.[10]

I. THE VIRTUAL BORDER FOR ELECTRONIC SURVEILLANCE PURPOSES

Instead of considering the physical regulation of virtual activities, in this essay I consider how a virtual border regulates physical activities. In particular, I consider how the law has created intangible borders to regulate government surveillance of communications. These intangible borders function the same way as physical borders functioned historically. They demarcate those "places" in which our government imposes burdens and grants privileges from those "foreign places" in which it does neither.[11] In this essay, I focus on the requirements imposed by the Fourth Amendment, under which government agents interested in monitoring communications must comply with a set of demanding procedures. As I will discuss, when the Fourth Amendment applies, it requires extensive judicial oversight of government surveillance investigations, before, during and after the surveillance takes place.[12]

The Fourth Amendment does not protect everyone, however. It mandates the greatest judicial oversight when

---

applied to" the Internet).

[9] *See, e.g.*, Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123-24 (W.D. Pa. 1997) (proposing a new sliding scale test for determining jurisdiction in cyberspace); Intel Corp. v. Hamidi, 71 P.3d 296, 302-12 (Cal. 2003) (resolving how the trespass to chattels doctrine applies to bulk e-mails sent by a disgruntled employee to his former employer).

[10] However, the exercise of sovereignty over foreigners whose online actions affect local residents remains the subject of considerable debate. *See, e.g.*, Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc) (dismissing on jurisdictional grounds a case that considered whether French parties' could enforce a domestic judgment against an American company whose web services in France were found to violate French law).

[11] In this context, I mean that our laws do not directly regulate the conduct of foreign persons in foreign countries, not that our practices impose no burdens on them.

[12] *See infra* Part II.A.

government agents monitor, for law enforcement purposes, the communications of "U.S. Persons"[13] in America.[14] At the opposite end of the spectrum, the Fourth Amendment has nothing to say about government surveillance of the communications of foreign persons in foreign places to gather foreign intelligence.[15] When they want to monitor entirely "foreign" communications, executive branch agents enjoy considerable discretion. That is in part because such surveillance falls within the executive's constitutional power to conduct foreign affairs,[16] and in part because foreigners surveilled abroad generally lack standing to bring cases in United States courts.[17] As the Fourth Circuit has noted, "[j]ust as the separation of powers . . . forced the executive to recognize a judicial role when the President conducts domestic security surveillance, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance."[18]

The executive's decision whether to monitor foreigners abroad derives from its foreign policy prerogatives, which the President exercises subject to limited involvement by the other two branches.[19] While the Senate approves of diplomats and

---

[13] Under Fourth Amendment doctrine, U.S. citizens and aliens with "sufficient connection with this country to be considered part of th[is] community" have the same rights. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). Federal statutory law refers to American citizens and permanent resident aliens as "U.S. Person[s]." 50 U.S.C. §§ 1801(i), 1821(1) (2005). Throughout this essay, the term "U.S. Persons" will be used to represent the group of citizens and aliens who have Fourth Amendment rights.

[14] *See infra* Part II.A.2.

[15] *See infra* Part II.B.1.

[16] *See, e.g.*, United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 319 (1936) (discussing the President's foreign affairs powers); *see also* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case*, 41 U.C. DAVIS L. REV. 1259 (2008) (describing and critiquing the foreign affairs argument for the President to have the power to conduct warrantless electronic surveillance for foreign intelligence).

[17] *See infra* Part II.B.1.

[18] United States v. Hung, 629 F.2d 908, 914 (4th Cir. 1980) (citation omitted).

[19] *See Curtiss-Wright*, 299 U.S. at 318. As I will discuss, when government agents cannot monitor foreigners without at the same time monitoring U.S. Persons, then the Fourth Amendment comes into play. *See infra* Part III.

consents to treaties and Congress controls military funding, the President alone decides whether to recognize foreign governments and what type of foreign relations to establish.[20] The executive branch's portfolio includes the monitoring of foreigners' communications abroad. Part of the foreign affairs function includes deciding whether to gather such intelligence in the first place and what to do with it if it is obtained.[21]

That a member of the judiciary must be intimately involved in purely domestic surveillance for violations of domestic crimes and that the executive branch has discretion over purely foreign surveillance of foreign people in foreign places seems clear.[22] But many, if not most, surveillance operations are neither purely domestic nor purely foreign, which substantially complicates the analysis. In fact, regulation of government surveillance of communications depends on so many factors that the rules Congress has formulated to handle them seem almost impenetrably complex.[23]

The pertinent statutory provisions may be found in the Foreign Intelligence Surveillance Act ("FISA").[24] Those rules currently grant more discretion to executive branch monitors when (1) the purpose of the investigation is to gather foreign intelligence information rather than information pertaining to criminal offenses, (2) the target of the surveillance is located in a

---

[20] That is not to say that the scope of the President's foreign affairs prerogatives may not be contested by both courts and Congress.

[21] I do not wish to minimize the enormity of the questions posed by surveillance of mixed domestic and foreign targets, but rather to suggest that some investigations are in fact purely across the virtual border. For further discussion of the problem of foreign surveillance investigations that target foreigners but end up listening in on Americans, see *infra* Part III.

[22] *See, e.g.*, *Hung*, 629 F.2d at 908 (describing the different considerations attendant to foreign intelligence surveillance and domestic criminal investigations).

[23] *See, e.g.*, Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 628-29 (2007) (describing "the fabled complexity of the [modern electronic surveillance statute] and the difficulty of applying it to new technologies" (footnote omitted)); Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283 (2005) (describing how modern electronic surveillance law handles spyware and identifying several points of complexity and uncertainty).

[24] *See* Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

foreign country rather than in the United States, (3) the monitoring itself is conducted in a foreign place rather than in the United States, (4) the target is a foreign citizen rather than a U.S. citizen or a resident alien, (5) the U.S. Person targeted communicates with someone in a foreign country rather than here, (6) there is probable cause to believe that the U.S. Person targeted is an agent of a foreign power rather than there being no association between the target and a foreign power.[25] Any one scenario involves some combination of the above pairings, which makes it even more difficult to determine the correct rule.

While the FISA scheme is a creature of Congress, it must conform to constitutional constraints.[26] As Part II discusses, Fourth Amendment precedents require the judiciary to oversee executive branch surveillance of purely "domestic" surveillance.[27] But the Fourth Amendment has much less, if anything, to say about executive branch conduct of purely "foreign" surveillance.[28] One could defensibly arrange the scenarios along a spectrum from most "domestic," and therefore protected by the Fourth Amendment, to most "foreign," and therefore least protected.

Rather than viewing the Fourth Amendment as providing decreasing judicial oversight as the character of the electronic surveillance becomes increasingly foreign, however, one could instead view Fourth Amendment protection as being all or nothing. In other words, one could view the Fourth Amendment as providing strict regulation for purely domestic investigations

---

[25] *See generally* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, § 11:2 (2007) (detailing the applicable statutory provisions).

[26] Note that the most recent amendments to FISA have been challenged in court for violating the First and Fourth Amendments and separation of powers. *See* Complaint at 3, 42, Amnesty Int'l USA v. McConnell, No. 08 CV 06259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf. On the other hand, the Bush administration has challenged FISA itself as an unconstitutional intrusion on the President's inherent authority as commander-in-chief. *See* ACLU v. NSA, 438 F. Supp. 2d 754, 780 (E.D. Mich. 2006) (rejecting government's claim that the executive branch had "inherent power" to conduct warrantless surveillance of international communications).

[27] *See infra* Part II.C.

[28] *See infra* Part II.B.

and no regulation for purely foreign investigations because the latter are governed by executive branch discretion. Then one would view the rules for cases that fall in the middle as designed to determine whether to treat the investigation as domestic or foreign. Under this view, in cases that are neither clearly domestic nor clearly foreign, the judge's role would be to review the executive's decision to deprive the target of judicial oversight of the surveillance that the Fourth Amendment mandates. The executive makes such a determination when a target effectively acts in the interest of a foreign power; in such a case, the executive may be said to "exile" that target if she is a U.S. Person.[29]

In this analysis, the virtual border plays a key role. On this side of the virtual border, domestic targets enjoy extensive judicial review of executive branch surveillance, pursuant to the dictates of the Fourth Amendment.[30] On the other side, foreign targets are subject to whatever electronic surveillance the executive branch chooses to conduct in the exercise of its foreign affair powers.[31] Foreign targets have no right to complain about surveillance techniques in our courts, though they may of course raise their complaints in their own courts.[32]

That is not to say that judicial review over mixed domestic and foreign cases is not mandated by the Fourth Amendment, but rather that judicial oversight in these cases plays an additional role besides keeping electronic surveillance within permissible bounds. In addition, judges review the executive

---

[29] *See infra* Part II.C (describing the FISA rules that regulate "exiling").

[30] *See infra* Part II.A, III.

[31] This is the case until the executive effectively brings them back over the border by prosecuting them, at which time the investigation becomes more like a domestic law enforcement investigation. *See, e.g.*, United States v. Hung, 629 F.2d 908, 914 (4th Cir. 1980) (discussing how the Fourth Amendment rights of the target change at the point that the investigation becomes "primarily" about law enforcement instead of foreign intelligence gathering). *But see* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006) (noting concern that past attempts to distinguish between foreign intelligence and law enforcement investigations, based in part on the *Hung* case, inhibited cooperation between executive branch agents).

[32] *See, e.g.*, Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 153 (D.D.C. 1976) (holding that an Austrian citizen subject to electronic surveillance by U.S. Army personnel in Berlin had no standing to sue in U.S. courts).

branch's decision to exile and ensure that U.S. Persons are not deprived of their Fourth Amendment rights either by being exiled over the virtual border without sufficient cause, or by being swept up in the surveillance of exiled U.S. Persons and foreigners.[33] The Fourth Amendment also calls for admitting foreign people inside our virtual border in some cases. For example, resident aliens and those with sufficient connections to this country who are targeted in ordinary criminal investigations benefit from the highest level of Fourth Amendment protection of their communications, even though they are not American citizens.[34]

By viewing the Fourth Amendment regulation of electronic surveillance as "on" for surveillance of people on the domestic side of the virtual border and "off" for those on the foreign side of the border, one can get a clearer view of how much is at stake in the "exiling decision." With that in mind, one can appreciate the importance of judicial oversight of the executive's decision to exile and can assess the rules governing that decision by how well they protect against improper exile.[35] Again, while one may view judicial review in these cases as quasi-constitutional Fourth Amendment protection,[36] one should also evaluate the judiciary's performance of its responsibility to oversee the exiling decision.

As mentioned, FISA contains the rules that determine the

---

[33] The surveillance of U.S. Persons who had not been "exiled" during the course of targeting those on the other side of the virtual border has caused considerable controversy in recent years in the wake of revelations about extensive surveillance by the NSA pursuant to a program called the "Terrorist Surveillance Program" ("TSP"). *See infra* note 146; *see also infra* Part III (discussing that controversy and Congress' response).

[34] *See infra* Part II.C.2 (discussing the "naturalization" process).

[35] For example, one could criticize the rules pertaining to electronic surveillance of the Internet as providing insufficient judicial oversight of the executive's decision to deprive cyber-citizens of Fourth Amendment rights. Under my formulation, the executive would be effectively exiling cybercitizens without a sufficient demonstration of "foreign" conduct. A full discussion of that problem is beyond the scope of this essay.

[36] *See, e.g.*, Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 458-59 (2005) (describing the FISA procedures as "quasi-constitutional" but casting doubt on the constitutionality of recent amendments).

amount of review provided by a judge over the exiling decision.[37] As will be discussed in Part II, those rules permit the executive branch to use special procedures that accord meaningfully fewer rights to foreign targets.[38] Foreign targets include those who are neither American citizens nor resident aliens (which together constitute "U.S. Persons"). But such targets also include those U.S. Persons who have effectively become foreigners through virtual exile. To exile a U.S. Person across the virtual border, high level executive branch officials must have probable cause to believe that the U.S. Person targeted for exile works as an "[a]gent of a foreign power,"[39] and the officials must seek "foreign intelligence information"[40] about that agent. If a reviewing judge approves the executive branch's showing, agents may conduct surveillance of the exiled target without according her the full Fourth Amendment rights granted to domestic targets.[41]

Importantly, and unlike in the domestic context, the "exiled" target does not have to receive notification of the surveillance unless and until the executive decides to bring criminal charges against the target based on the evidence gathered.[42] The lack of notice enhances the executive's discretion to conduct surveillance of exiled people, because it reduces the likelihood that the executive's decision to exile and its surveillance thereafter will face a challenge in court.[43] As I mentioned earlier and will further discuss, on this side of the virtual border, where full Fourth Amendment rights apply, judges must actively keep executive branch surveillance within prescribed bounds throughout all phases of the investigation and must provide notice to the target when the surveillance

---

[37] *See* Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[38] *See infra* Part II.B.

[39] 50 U.S.C. § 1801(b) (Westlaw through July 2008 amendments).

[40] § 1804(a)(7)(B) (2000).

[41] *See infra* Part II.C.

[42] *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1039 (D. Or. 2007).

[43] *See infra* text accompanying notes 145-156 (discussing the difficulty of bringing cases challenging FISA surveillance).

concludes.[44]

The FISA rules require a judge to review the executive's decision to exile a U.S. Person across the virtual border.[45] Because a U.S. Person loses a significant constitutional right—the right to substantial judicial oversight of executive branch surveillance—when she is exiled across the virtual border, the banishment decision must not be made lightly. The executive branch cannot be trusted to make those decisions unfettered because it would have an incentive to treat all U.S. Persons as foreigners, merely to avoid Fourth Amendment constraints.[46] History amply demonstrates that executive branch agents find it tempting to move as many people across the virtual border as possible in order to avoid penetrating judicial oversight.[47]

A special court, the Foreign Intelligence Surveillance Court ("FISC") oversees the executive branch's attempts to exile U.S. Persons over the virtual border.[48] The FISC operates in private, ex parte, and generally without publishing its decisions in order to protect the secrecy of the executive branch's counterintelligence and counterterrorism operations.[49] When the FISC reviews the executive branch's claims that a U.S. Person has been acting sufficiently "foreign" to justify exile, it operates as an essential check on executive discretion.[50]

In this essay, I develop the concept of the virtual border and

---

[44] *See infra* Part II.A.1.

[45] *See infra* Part II.C.1 (discussing specifics of the FISA rules).

[46] Although FISA procedures do accord some protections that are similar to those provided to domestic targets, such as the minimization requirement, it is not clear that those protections are constitutionally mandated. *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002). In addition, my point is not that the FISA procedures for judicial review do not accord rights, but that their function is meaningfully different from the function served by judicial review of executive branch surveillance in the domestic context.

[47] *See generally* KRIS & WILSON, *supra* note 25, Chap. 3 (recounting how history of executive branch abuses of surveillance powers spurred congressional regulation); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004); *see also infra* Part III (discussing implications of tendency for executive branch to abuse surveillance powers).

[48] *See* 50 U.S.C. § 1803 (Westlaw through July 2008 amendments).

[49] Bellia, *supra* note 36, at 460-74 (arguing for greater transparency surrounding the proceedings of the FISC).

[50] See *infra* Part II.C.1 for a full discussion of the FISA procedures.

illustrate how the FISA rules are designed to ensure U.S. Persons are not improperly deprived of their Fourth Amendment rights by exile. The goal is to provide a new way to evaluate the foreign surveillance laws based on whether they provide adequate judicial review of the executive's decision to exile. In recent years, for example, the foreign surveillance rules have been both amended and flouted in ways that weaken this essential function.

Because this paper aims to promote an understanding of how the electronic surveillance laws are supposed to function, it focuses first and most thoroughly on how they are designed to work under applicable constitutional precedents rather than how they have been significantly altered by recent amendments or ignored altogether.[51]

Part IIA of this essay discusses the Fourth Amendment precedents that establish who is on this side of the virtual border and the extensive judicial review accorded to government surveillance of those people. Then, Part IIB reviews the Fourth Amendment precedents that establish who is on the other side of the virtual border, whether they are physically located outside of this country or not.[52]

In Part IIC, I describe how FISA requires that government agents interested in conducting electronic surveillance of U.S. Persons have to convince a judge that they are seeking foreign intelligence information about targets who are agents of a foreign power before they may deprive those targets of their Fourth Amendment rights. As a result, U.S. Persons in this country enjoy either the protections of full judicial review of executive branch surveillance, or judicial oversight of the determination to exile them over the virtual border where they

---

[51] A more extensive analysis of the ways in which the current executive branch abuses reflect insufficient judicial oversight of the exiling decision is planned for a subsequent paper.

[52] Because this essay considers the border between domestic criminal cases and foreign cases, it does not inquire into state surveillance laws. For a thorough and important discussion of wiretapping at the state level, see Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L. J. 971 (2003).

no longer benefit from those protections.[53]

Part III of this essay considers recent changes and challenges to judicial review of the exiling decision. In the past several years, the FISA rules have expanded executive branch discretion in ways that dramatically weaken judicial oversight of the exiling decision.[54] At the same time, officials in the Bush administration appear to have extensively abused their electronic surveillance tools in the wake of the tragic attacks on September 11, 2001, by exiling U.S. Persons with insufficient justification.[55] Finally, recent practices of all three branches have made it difficult for challenges to the exiling process to be heard in court. [56]

The reality of executive branch overreaching reinforces the need for extensive judicial review of electronic surveillance on this side of the virtual border as well as effective judicial review of executive branch decisions to exile people across the virtual border. But while executive branch abuse of electronic surveillance has been egregious during the Bush administration,[57] it threatens to persist afterwards if members of the judiciary play an unduly circumscribed role in overseeing executive actions.

---

[53] Here I am using the formulation under which one has all Fourth Amendment rights in the domestic context and none over the virtual border.

[54] *See infra* Part III.

[55] *See, e.g.*, JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2008) (detailing extensive NSA surveillance of Americans without obtaining the requisite judicial review); Hepting v. AT & T Corp., 439 F. Supp. 2d 974, 992-94 (N.D. Cal. 2006) (considering class action claim against large telecommunications company for aiding the NSA in conducting illegal surveillance); Curtis Bradley et. al., *On NSA Spying: A Letter to Congress*, 53 N.Y. REV. OF BOOKS 2 (2006), *available at* http://www.nybooks.com/articles/18650.

[56] *See, e.g.,* FISA Amendments Act of 2008, Pub. L. No. 110-261,122 Stat. 2436 (providing for courts to dismiss pending and future actions challenging any assistance provided to the "President's Surveillance Program" or "Terrorist Surveillance Program" if the Attorney General certifies that the assistance was authorized by the President to detect, prevent, or prepare for a terrorist attack).

[57] *See, e.g.*, JAMES X. DEMPSEY & DAVID COLE, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY (2d ed. 2002); KRIS & WILSON, *supra* note 25; Swire, *supra* note 47, at 1325-29.

II. ESTABLISHING THE VIRTUAL BORDER

A. On this Side of the Virtual Border

1. Rigorous Judicial Review of Electronic Surveillance Investigations

When the government uses electronic surveillance to monitor communications, it significantly intrudes on privacy.[58] While a consensus on what "privacy" is remains elusive, there is no doubt that when the government listens in on its citizens' communications, it violates their privacy by inhibiting their right to be let alone and by raising the risk that they will face negative consequences for their speech.[59] Supreme Court Justices have historically taken a jaundiced view of government surveillance of communications, with some regarding it as a "dirty business,"[60] and others recognizing that there is perhaps no greater threat to freedom than that posed by government surveillance of our communications.[61] As Justice Powell wrote in 1972, "[t]here is, understandably, a deep-seated uneasiness and apprehension that th[e] [electronic surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens."[62]

Electronic surveillance does, however, provide government agents with a powerful investigative tool.[63] More than fifty

---

[58] *See generally* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 95 (2000) (describing both the privacy intrusions inherent in electronic surveillance by government and the history of legal regulation of such surveillance).

[59] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972); *see also* Maclin, *supra* note 16, at 1285-87.

[60] Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

[61] *See, e.g.*, Berger v. New York, 388 U.S. 41, 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."); Lopez v. United States, 373 U.S. 427, 470 (1963) (Brennan, J., dissenting) ("If electronic surveillance by government becomes sufficiently widespread, and there is little prospect for checking it, the hazard that as a people we may become hagridden and furtive is not fantasy.").

[62] *Keith*, 407 U.S. at 312.

[63] *See, e.g.*, *id.* at 311-12 ("The covertness and complexity of potential unlawful

years ago, advocates for electronic surveillance argued that the dramatic rise in organized crime and the difficulty of infiltrating its networks with informants or undercover agents mandated law enforcement use of electronic surveillance.[64] By 1968, a sufficient consensus had emerged for Congress to pass the Wiretap Act,[65] according to which government agents could use electronic surveillance to investigate crimes, subject to a set of stringent procedural requirements. Those limitations came directly from two Supreme Court cases decided the prior year.

In the landmark cases of *Katz v. United States*[66] and *Berger v. New York*,[67] the Supreme Court recognized the strength of the law enforcement rationale for permitting some investigative use of electronic surveillance by the government.[68] At the same time, the Supreme Court emphasized in both cases the considerable risk to privacy posed by electronic surveillance of our communications.[69] For that reason, the Court refused to let the executive branch determine for itself whether sufficient cause justified its use of electronic surveillance and the Court refused to "retroactively validate" the government's conduct, because agents had proceeded without "prior judicial sanction."[70] Thus, the *Katz* Court found the executive branch's interception

---

conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances.").

[64] *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 15-42 (2004) (reviewing the history of the passage of the Wiretap Act).

[65] Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351, 82 Stat. 212, (codified as amended in scattered sections of 18 U.S.C. §§) (1968) ("Wiretap Act"). Prior to the passage of the Wiretap Act, twenty-one members of the Senate supported a bill to permit electronic surveillance by government agents to protect national security, but not for ordinary crime control. *See* S. REP. NO. 90-1097, at 161 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2223.

[66] 389 U.S. 347 (1967).

[67] 388 U.S. 41 (1967).

[68] *See id.* at 63.

[69] *See id.* at 56; *Katz*, 389 U.S. at 353.

[70] *Katz*, 389 U.S. at 356; *see also id.* at 356-57 ("[The Supreme] Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.").

of the contents of the target's telephone call to violate the Fourth Amendment because the government had neither obtained a prior warrant nor established an exception to the warrant requirement.[71] The Court emphasized that "subject only to a few specifically established and well-delineated exceptions," none of which would likely apply to electronic surveillance, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment."[72]

In *Berger*, the Supreme Court provided more guidance about what the Fourth Amendment requires when it struck down a New York statute that authorized law enforcement use of electronic surveillance.[73] The Court identified some of the features of electronic surveillance that necessitated close judicial review of its use. The Court noted that because electronic surveillance, as compared to a traditional search of a house, is hidden, continuous, intrusive, and indiscriminate, it poses a heightened threat to the target's privacy.[74] The Court opined that absent "adequate judicial supervision" executive branch use of electronic surveillance devolved into the general warrant that the Framers clearly proscribed as a violation of the Fourth Amendment.[75] To properly reduce the risks and intrusion inherent in electronic surveillance, the Court enunciated several procedural requirements with which executive branch officials must comply before they may engage in electronic surveillance.[76]

The *Berger* Court's requirements, which Congress codified in the 1968 Wiretap Act,[77] are all designed to ensure that

---

[71] *Id.* at 358.

[72] *Id.* at 357.

[73] *See Berger*, 388 U.S. at 57-60.

[74] *See id.* at 59-60; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 10-11. *See also id.* at ¶¶ 50-56 (discussing how courts made the same findings regarding video surveillance and applied the core features of the Wiretap Act to that practice as a matter of Fourth Amendment law).

[75] *Berger*, 388 U.S. at 60.

[76] *Id.* at 63.

[77] Note that there is some dispute about just which of the requirements in the Wiretap Act are constitutionally required. *See, e.g.*, United States v. Koyomejian, 970 F.2d 536, 542-51 (9th Cir. 1992) (en banc) (Kozinski, J., concurring).

surveillance is used only in those cases in which executive branch agents may demonstrate a strong need to a court, prior to initiating the surveillance. In the Act, Congress requires a tight nexus between the target of the search and probable cause to believe that the target is engaged in a serious crime, as well as specificity regarding which conversations investigators seek.[78] In addition, agents have to establish that less intrusive methods of investigation are not possible.[79] Courts also oversee the surveillance while it takes place by requiring that agents report periodically on their progress and minimize the interception of non-incriminating conversations.[80] After the electronic surveillance ends, courts review submitted transcripts to determine whom, besides the target, should receive notice.[81] Courts hear claims by those surveilled that agents acted illegally and grant the exclusion of evidence, as well as damages, when those claims are successful.[82] In sum, the Fourth Amendment, as codified in the Wiretap Act, requires executive branch agents to submit to rigorous judicial oversight before, during and after their use of electronic surveillance to investigate.

2. Clear Residents: U.S. Persons Suspected of Domestic Crimes

The cases that established the requirements of rigorous judicial oversight, *Berger* and *Katz*, involved law enforcement investigations of U.S. citizens suspected of domestic crimes. In other words, the targets in those cases did not even arguably fall within the foreign affairs concerns of the executive branch.[83] Subsequent cases and statutory provisions have addressed what to do in cases that implicate both foreign affairs and Fourth Amendment rights, but all have taken for granted that

---

[78] *See* Freiwald, *supra* note 64, at 23-26 (reviewing the Wiretap Act requirements).

[79] 18 U.S.C. § 2518(3)(c) (2006).

[80] § 2518(5).

[81] § 2518(8)(d).

[82] § 2515.

[83] *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308 (1972) (describing the *Berger* and *Katz* cases as involving "the surveillance of crimes unrelated to the national security interest").

electronic surveillance within this country by domestic law enforcement of citizens may proceed only by meeting the heightened requirements set out in *Berger* and *Katz* and codified in the Wiretap Act.

3. U.S. Persons Threatening Domestic Security Are Also Residents

An important question that neither *Berger* nor *Katz* resolved was what power the President retained to conduct surveillance without meeting the requirements set out in those two cases.[84] Apparently, presidents had been authorizing warrantless electronic surveillance based on the need to protect the national security for decades prior to passage of the Wiretap Act, and they continued to do so after 1968.[85] The Wiretap Act did not address that executive practice, but instead specifically declined to "limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."[86]

In *Keith*, the Supreme Court considered a challenge by a domestic group which the Attorney General viewed as a "national security" threat to the executive branch's warrantless surveillance of its communications.[87] The executive branch supported its practices on the ground that it needed more leeway to investigate threats to national security because such threats required specialized and secretive intelligence techniques that varied meaningfully from those used in

---

[84] *See* Katz v. United States, 389 U.S. 347, 358 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

[85] *See Keith*, 407 U.S. at 299 ("Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees . . . ."(footnote omitted)); *see also id.* at 310 n.10; Bellia, *supra* note 36, at 430-31 (reviewing history).

[86] 18 U.S.C. § 2511(3) (1972) (amended 1978).

[87] *Keith*, 407 U.S. at 300-01; *see generally* Maclin, *supra* note 16, at 1279-320 (discussing the background to the *Keith* case and its modern applicability).

investigations of ordinary crimes.[88] According to the Attorney General, the surveillance of the defendants had been "'necessary to protect the nation from attempts . . . to attack and subvert the existing structure of Government.'"[89]

Before turning to the merits of the constitutional claim, the Supreme Court rejected the government's claim that the Wiretap Act's language specifically authorized the executive to conduct warrantless surveillance to protect national security.[90] The Court found that in the Wiretap Act, Congress had "simply left presidential powers where it found them."[91]

Having dispensed with the statutory argument, the Supreme Court recognized the perennial conflict between the executive branch's desire to conduct surveillance without submitting to rigorous judicial review, and the constitutional requirement that the judiciary retain an active role in keeping such surveillance within defensible limits to protect citizens' rights. The Court formulated its task as "examin[ing] and balanc[ing] the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."[92]

Ultimately, the Court determined that, while the executive's compelling interest in protecting the country against domestic threats does exceed its interest in enforcing the criminal laws, subjecting national security surveillance to a Fourth Amendment warrant requirement would not "unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it."[93] Moreover, the Court decided that because "Fourth Amendment freedoms [could not] properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive

---

[88] *Keith*, 407 U.S. at 318-19.

[89] *Id.* at 309 (quoting the Attorney General's affidavit).

[90] *Id.* at 303.

[91] *Id.* Congress eventually removed the provision in the Wiretap Act that the government had relied on to claim Congressional approval of its actions in *Keith*.

[92] *Id.* at 314-15.

[93] *Id.* at 315; *see also id.* at 320-21.

Branch," investigators and prosecutors could "not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[94] Under the Court's reasoning, even their participation in activities that threaten the very existence of their country is insufficient justification to exile Americans across the virtual border where they would be deprived of rigorous judicial oversight of law enforcement surveillance.

Interestingly, the Supreme Court emphasized that both Fourth Amendment and First Amendment values supported subjecting executive branch surveillance practices to rigorous judicial oversight. The Court recognized that the executive branch would necessarily cast a suspicious eye on those who espoused views contrary to its programs and policies, and would be inclined to view such actors as posing a threat to "domestic security."[95] But if such suspicions were sufficient to justify the use of so intrusive a technique as electronic surveillance, that would pose a serious threat to citizens' ability to exercise their First Amendment rights of assembly and speech. Speakers might refrain from criticizing the executive branch for fear of surveillance and retaliation, in direct contradiction of core constitutional values. As the Court dramatically expressed it:

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[96]

The *Keith* Court affirmed the need for "[p]rior review by a neutral and detached magistrate" of the executive's decision to use electronic surveillance.[97] The Court required executive

---

[94] *Id.* at 316-17.

[95] *See id.* at 314 ("History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies.").

[96] *Id.* at 314.

[97] *Id.* at 318. The Court ruled that reliance on "post-surveillance judicial review" alone would be insufficient. *Id.* The Court clearly contemplated judicial review both before and after the surveillance took place. *Id.* at 321.

branch agents to submit to the requirements of prior judicial review whenever they sought to investigate U.S. Persons for violation of our laws, unless those U.S. Persons were suspected of having a "significant connection with a foreign power, its agents or agencies."[98]

The Court recognized that different procedures could apply in cases involving domestic security rather than ordinary crime because of differences in purposes and methods.[99] In particular, the Court suggested that the greater need for secrecy in investigations might require that surveillance applications be made to a member of a specially designated court; that the difficulty in identifying the exact targets might require a different standard than the probable cause standard in the Wiretap Act; and that the more long-range and preventative nature of the investigation could support longer time periods and less stringent reporting requirements.[100] However, the Court refused to excuse the executive branch from obtaining prior judicial approval when it used electronic surveillance to investigate U.S. Persons.[101]

Congress might have responded to the *Keith* decision by drafting a special set of procedures for surveillance of U.S. Persons suspected of domestic terrorism, or domestic threats to national security. Had it done so, the procedures could have been a watered-down, or at least adjusted, set of Fourth Amendment requirements pursuant to the *Keith* Court's recognition that procedures less rigorous than those under the Wiretap Act could regulate such cases.[102] But Congress did not do that.[103]

Instead, Congress accepted the Court's invitation to draft special rules, but designed them to apply only in situations

---

[98] *See id.* at 309, n.8 (defining "domestic organizations" as having no such connections).

[99] *Id.* at 322-23.

[100] *Id.*

[101] *Id.*

[102] *See id.*; Banks & Bowman, *supra* note 58, at 52-53.

[103] *See generally* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 803 (1989) (describing the passage and provisions in FISA).

involving foreign powers and their agents. The procedures codified in FISA provide for the FISC to hear claims brought by the executive branch that the target of its surveillance efforts is either a foreign power or an agent of a foreign power, and that the executive seeks "foreign intelligence information" about that target.[104] So while Congress presumably could have provided a different, and somewhat more lenient, set of procedures for those cases when the government investigated Americans viewed as threats to national security, instead it required that American targets become more foreign before they may be targeted using the FISA procedures.[105]

To summarize, participation in activities viewed by the executive branch as threats to national security is insufficient to exile a U.S. Person over the virtual border to the place where the executive branch has more discretion to conduct surveillance pursuant to its power over foreign affairs. Instead of drawing a line solely based on the nature of the threat, FISA draws the line based on the "foreignness" of the target investigated. At some point a U.S. Person's foreign conduct is enough to exile that person over the virtual border into a "foreign land" of executive discretion rather than judicial oversight of their surveillance.

4. U.S. Citizens Abroad

U.S. citizens enjoy some Fourth Amendment protection of their communications even when they are outside the physical confines of the United States.[106] This further illustrates the

---

[104] 50 U.S.C. § 1801(e) (2006).

[105] *See* Banks & Bowman, *supra* note 58, at 95 (noting anomaly that U.S. Persons targeted in domestic terrorism investigations are subject to the same procedures as such persons targeted for violation of U.S. crimes, despite the fact that the domestic terror threat may be just as great as the foreign terror threat).

[106] Reid v. Covert, 354 U.S. 1, 5 (1957) ("[W]e reject the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights."); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 160 (D.D.C. 1976) (noting requirement that federal officials "present for approval in the United States a warrant for a wiretap [of an American citizen] overseas"). In a decision issued just as this essay was going to press, the Second Circuit recognized the Fourth Amendment rights of U.S. citizens surveilled abroad by U.S. agents, but interpreted those rights to require reasonableness

virtual, rather than physical, nature of the border that separates the area in which targets are subject to the protections of the Fourth Amendment from the foreign space in which they are not. In one case, *Berlin Democratic Club v. Rumsfeld*, the court considered the Fourth Amendment rights of "a number of American citizens and organizations and one Austrian citizen" living in Berlin who claimed they were subject to an extensive campaign of illegal electronic surveillance and harassment by the U.S. Army.[107] Based on the *Keith* decision, the court found that the Fourth Amendment compelled government investigations to obtain judicial authorization prior to conducting electronic surveillance of the Americans living in Berlin.[108] It is important to note that the court found that even though the American citizens and their organizations were overseas, there was "no evidence of collaboration with or action on behalf of a foreign power."[109] Thus, when U.S. agents monitor "domestic" U.S. citizens abroad, they do so subject to the protections of the Fourth Amendment.[110] By leaving U.S. territory, American citizens do not automatically leave the protections of the Fourth Amendment behind.

B. On the Other Side of the Virtual Border

1. Foreigners Abroad

Because the Supreme Court necessarily stays out of cases that fall clearly within the foreign affairs power of the President

---

rather than a warrant. See United States v. Odeh (*In re* Terrorist Bombings of U.S. Embassies in East Africa (Fourth Amendment Challenges)), 548 F.3d 276, (2d Cir. 2008).

[107] *See Berlin Democratic Club*, 410 F. Supp. at 147-48.

[108] *See id.* at 156-57.

[109] *See id.* at 159.

[110] See *id.* at 156-57. Note that the Justices have not entirely agreed about just what the Constitution requires when applied abroad. *See, e.g.*, *Reid*, 354 U.S. at 74 (Harlan, J., concurring) (disagreeing with the notion that "every provision of the Constitution must always be deemed automatically applicable to American citizens in every part of the world"); *but see id.* at 8-9 (majority opinion) ("While it has been suggested that only those constitutional rights which are 'fundamental' protect Americans abroad, we can find no warrant, in logic or otherwise, for picking and choosing among the remarkable collection of [constitutional] 'Thou shalt nots' . . . ." (footnote omitted)).

and because of jurisdictional issues, few cases squarely address the Constitutional rights of foreign people in foreign places. In the *Berlin Democratic Club* case described above, the court found that the Austrian citizen, who was apparently subject to the same electronic surveillance as the Americans, could not bring a claim. The Austrian citizen lacked standing to sue because, as a "citizen of a foreign country," he was "not subjected to the laws of this country" and he could "utilize the laws of his own country to protect himself."[111]

Foreign citizens may not generally complain in U.S. courts when our government conducts surveillance of them outside this country. Congress has some power over the executive branch's foreign surveillance through its power of the purse,[112] and the executive may face both domestic and foreign challenges to whatever surveillance practices become known.[113] But when the surveillance monitors purely foreign citizens in foreign countries, it is beyond the power of the U.S. courts to address. What makes government surveillance in foreign places of foreign people constitutionally controversial is the substantial risk that U.S. Persons will be caught up in the monitoring, which is a problem discussed in Part III.

2. Foreigners Here but Without Sufficient Connection

The story is different when the foreigner bases his claims to Fourth Amendment protections on some connection to the United States, which could be either the foreigner's presence here when surveilled or his prosecution here. These cases help illustrate the virtual border between those targets subject to rigorous judicial review under the Fourth Amendment and those

---

[111] *Berlin Democratic Club*, 410 F. Supp. at 153. The court noted that it would have been different if the United States had tried to prosecute the Austrian citizen in the United States or if he had applied for relief under a U.S. statute that permits relief to a non-resident alien. *See id.* at 152.

[112] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 15 (1972) (noting that Congress, but not the courts, should monitor the "wisdom and soundness of Executive action").

[113] *See generally* BAMFORD, *supra* note 55 (reporting on NSA surveillance after the September 11 attacks); JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY (2001) (chronicling NSA surveillance efforts before September 11, 2001).

not so protected.

In the case of *United States v. Verdugo-Urquidez*,[114] the defendant sought to have evidence obtained during a search of his home in Mexico, conducted by U.S. agents in concert with Mexican officials, excluded from his trial in the United States on drug-trafficking charges. The Supreme Court found that the defendant's mere presence in the United States for trial was insufficient to entitle him to rights under the Fourth Amendment.[115] The Court distinguished precedents in which aliens had been granted constitutional rights as involving aliens who had "come within the territory of the United States and developed substantial connections with this country."[116] The Court based its decision in part on a reading of "the people" in the text of the Fourth Amendment.[117] The Court also expressed concern that recognizing Fourth Amendment rights in aliens abroad "could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."[118]

A subsequent case applied the reasoning in *Verdugo-Urquidez* to a case involving a Russian citizen suspected of computer hacking.[119] A federal district court held that the defendant, Gorshkov, could raise no Fourth Amendment complaint about a remote search of his computer in Russia, even though he had visited undercover officers in the United States as part of a sting operation.[120] The court found that "a single entry into the United States that is made for a criminal purpose is hardly the sort of voluntary association with this country that

---

[114] 494 U.S. 259 (1990).

[115] *Id.* at 271 (rejecting defendant's claim to Fourth Amendment protection on the ground that he was "an alien who has had no previous significant voluntary connection with the United States").

[116] *Id.*

[117] *Id.* at 265 ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." (quoting U.S. CONST. amend. IV)).

[118] *Id.* at 273-74.

[119] United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[120] *Id.* at *3.

should qualify Defendant as part of our national community for purposes of the Fourth Amendment."[121]

A person may come to qualify for Fourth Amendment protections only by actions which ground him sufficiently on this side of the virtual border, actions that neither Verdugo-Urquidez nor Gorshkov accomplished. These cases thus illustrate the difficulty for foreigners of getting over the virtual border into this country. Being here physically is not enough. The next section considers what is enough to move one onto the domestic side of the virtual border and what is enough to justify banishment.

C. Crossing the Virtual Border

1. Statutory Procedures for Border Movements

a. Of U.S. Persons

Under FISA, executive branch officials may not banish U.S. Persons across the virtual border without first convincing a judge of probable cause to believe the target is an agent of a foreign power and that other requirements have been met.[122] Before they may conduct surveillance of U.S. Persons, executive branch officials must submit a detailed application with affidavits from investigators, a certification from a high-ranking official and the Attorney General's approval.[123] The application must establish probable cause to believe that the target is an "agent of a foreign power" when the target is a U.S. Person.[124] That roughly means the target has engaged in spying for a

---

[121] *Id.*

[122] *See, e.g.*, KRIS & WILSON, *supra* note 25 (describing FISA procedures); Bellia, *supra* note 36, at 436-48 (same).

[123] *See* Kris, *supra* note 31, at 490 (citing 50 U.S.C. § 1804).

[124] 50 U.S.C. § 1804(a)(3)(A) (Westlaw through July 2008 amendments). The government must also show that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(B) (Westlaw through July 2008 amendments).

foreign power, sabotage or international terrorism.[125] After amendments made by the USA PATRIOT ACT ("Patriot Act"),[126] a U.S. Person may not be considered to be an agent of a foreign power based solely on speech or actions protected by the First Amendment.[127] Presumably that requirement reflects the Supreme Court's concern in *Keith* that the executive branch might make a claim of national security necessity to conduct surveillance actually designed to silence or harass unpopular views.[128]

The FISA procedures themselves require the FISC to review the executive's showing, but to accord it considerable deference. The FISC reviews both the claim that the target is an agent of a foreign power, and the executive branch's assertion that the proposed surveillance is designed to gather "foreign intelligence information."[129] The whole system operates on the premise that the executive requests permission to conduct surveillance free of the Wiretap Act requirements only when there is sufficient evidence to justify it, which is why FISC denial of executive branch requests is so rare.[130]

For those investigations in which the executive branch succeeds in having the FISA procedures apply rather than the Wiretap Act, the regulations differ considerably.[131] As

---

[125] § 1801(b); Kris, *supra* note 31, at 491-92.

[126] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272.

[127] *See* 50 U.S.C. § 1805(a)(2)(A) (2000 & Supp. 2001); 50 U.S.C. § 1842(a)(1) (2000 & Supp. 2001); KRIS & WILSON, *supra* note 25, at § 8:37; Bellia, *supra* note 36, at 447;

[128] *See supra* Part II.A.3. It is not altogether clear how this protection would be enforced, particularly in light of plaintiffs' standing problems in FISA cases. *See, e.g.*, *In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1131-35 (N.D. Cal. 2008) (illustrating the difficulty of establishing oneself as an "aggrieved person" under FISA when one cannot use evidence protected by states' secrets).

[129] § 1804(a)(6)(B).

[130] *See* Bellia, *supra* note 36, at 459 (reporting that between 1979 and 2006, only twenty-one of 17,000 FISC orders were challenged, and none of the challenges were successful). Of course it is possible that the judges on the FISC are loathe to second guess the executive's decision to exile because they view it as properly within the President's discretion. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) (discussing executive's discretion in the field of foreign affairs).

[131] *See* Banks & Bowman, *supra* note 58; Bellia, *supra* note 36, at 439-42.

previously discussed, agents who succeed in meeting the FISA requirements may conduct surveillance for longer periods, and they may refrain from giving notice to the target unless and until the target faces prosecution on criminal charges.[132]

FISA thus endeavors to ensure that the executive branch decision to exile a U.S. Person is not made lightly and is subject to review. The procedures, including review by a secret court and the accompanying limited public disclosure, balance the executive's need to have discretion over its foreign affairs power with the judiciary's duty to ensure that the Fourth Amendment has real meaning.

b. Of Foreign Persons

As discussed above, when foreign citizens have sufficient connection to the United States to fall under the umbrella of U.S. Persons, they are entitled to the Fourth Amendment protections of judicial review and are treated the same as a U.S. citizen. But those who lack that connection are not. FISA establishes detailed procedures for targets of surveillance who are not U.S. Persons, meaning they are neither citizens nor permanent residents, and those procedures accord significantly less protection.

Thus, the executive branch may conduct surveillance of non-U.S. Persons, under FISA, on a showing that they are linked to a foreign power.[133] It is easier to establish that the agent is seeking foreign intelligence information with regard to non-U.S. Persons, and the application is reviewed only for completeness rather than clear error.[134] In addition, unlike U.S. Persons suspected of foreign intelligence activities, foreigners in this country may be surveilled without any concern that First Amendment protected activities have provided the only basis for the surveillance.

---

[132] *Compare* Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding procedures dramatically different), *with In re* Sealed Case, 310 F.3d at 737-42 (finding procedures comparable).

[133] *See* 50 U.S.C. § 1801(b)(1) (Westlaw through July 2008 amendments); Kris, *supra* note 31, at 490-92.

[134] 50 U.S.C. § 1805(a)(4) (Westlaw through July 2008 amendments).

2. When the Fourth Amendment Requires Naturalization

Some non-resident aliens, even those monitored abroad, may acquire the right to bring Fourth Amendment challenges to their surveillance. In one scenario, those monitored abroad but then brought to the United States for prosecution have been found to have standing to bring Fourth Amendment challenges to their surveillance.[135] It is also possible that an alien abroad could somehow fit within the *Verdugo-Urquidez* test of having sufficient connection to the United States to raise a Fourth Amendment claim to U.S. government surveillance abroad.[136] Either way, the fact that foreign people subject to government surveillance abroad may, in some cases, bring a Fourth Amendment challenge to that surveillance reinforces the notion that the line dividing Fourth Amendment protected targets from those who are not is much more virtual than physical.

III. Recent Changes and Challenges to Judicial Review at the Virtual Border

Although the *Keith* Court recognized that the Fourth Amendment protections accorded to U.S. Persons who acted in concert with foreigners could differ dramatically from those targeted for domestic crimes and national security, it neither

---

[135] *See, e.g.*, United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974) (foreign citizen wiretapped abroad entitled to bring Fourth Amendment claim when the government sought to introduce evidence obtained thereby in a criminal case against him in the United States); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 152 (D.D.C. 1976) (stating as an exception to the general rule that non-resident aliens have no standing in United States courts: "when a non-resident alien is brought from abroad to appear for and be the subject of a domestic criminal prosecution"); *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 279 (1990) (Brennan, J., dissenting) (arguing that when government agents enforce U.S. criminal laws abroad, they do so subject to the Fourth Amendment).

[136] *See, e.g.*, Douglas I. Koff, *Post*-Verdugo-Urquidez*: The Sufficient Connection Test – Substantially Ambiguous, Substantially Unworkable*, 25 COLUM. HUM. RTS. L. REV. 435 (1994) (arguing in favor of an expansive approach to finding non-resident aliens searched abroad by U.S. government agents subject to the protections of the Fourth Amendment). *But see* Randall K. Miller, *The Limits of U.S. International Law Enforcement After Verdugo-Urquitez: Resurrecting Rochin*, 58 U. PITT. L. REV. 867, 885 (1997) (arguing that aliens outside the United States should have no protection under the Fourth Amendment).

defined what actions counted nor did it specify what protections, if any, would be accorded. As the Court wrote in *Keith*,

> No doubt there are cases where it will be difficult to distinguish between 'domestic' and 'foreign' unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case.[137]

Perhaps surprisingly, the question of exactly how the Fourth Amendment regulates foreign intelligence surveillance of U.S. Persons remains unanswered by the Supreme Court. Though some decisions issued in the period after *Keith* and before passage of FISA assumed that the President's power over foreign affairs included the right to conduct warrantless surveillance for foreign intelligence purposes, others questioned that proposition.[138] In a recent case issued by the Foreign Intelligence Surveillance Court of Review ("FISCR"), which met for the first time to consider whether the FISC had properly found amendments made by the Patriot Act to violate the Fourth Amendment, the FISCR opined that the constitutional question about how the Fourth Amendment regulates foreign intelligence surveillance remained unresolved both before and after it issued its decision.[139]

The FISCR's decision addressed whether FISA's procedures adequately ensured that agents did not follow FISA standards in cases more properly pursued as law enforcement investigations regulated by the Wiretap Act.[140] The FISCR concluded that the statute satisfied the Fourth Amendment, even though the new provisions permit agents to follow FISA procedures whenever a

---

[137] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 309 n.8 (1972).

[138] *Compare In re* Sealed Case, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) (recognizing precedents holding that the President had inherent executive authority to conduct warrantless foreign surveillance searches), *with* Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975) (en banc) (plurality opinion) (finding warrantless surveillance for foreign intelligence purposes to be constitutionally unreasonable). *See also* Bellia, *supra* note 36, at 435-36 (reviewing this history).

[139] *See In re* Sealed Case, 310 F.3d at 746.

[140] *See id.* at 737-46.

significant purpose of the investigation is to gather foreign intelligence information. Before the Patriot Act amendments, agents had to show that the primary purpose, instead of a significant purpose, was to gather foreign intelligence information.[141]

The FISCR's decision has generated significant criticism in academia, and a federal district court has specifically rejected it.[142] In *Mayfield v. United States,* the district court in Oregon held FISA, as amended, to be facially invalid under the Fourth Amendment because the provisions too easily permitted the executive branch to deprive a U.S. Person of full Fourth Amendment rights without a sufficient showing of probable cause.[143] Whether or not the *Mayfield* court's analysis stands up to review, the court addressed the conditions under which executive branch agents may exile U.S. Persons and expressed concern about the adequacy of the executive's showing.[144]

Both the FISCR and *Mayfield* opinions considered whether FISA's procedures provided adequate judicial oversight of the executive's showing to justify exile. Both illustrated that the decision to exile a person has significant implications for that person's rights, and that the exiling process itself must meet constitutional standards. However, both cases may rarely, if ever, be replicated, because of the difficulties involved in challenging exiling decisions.[145]

---

[141] *Id.* at 746. *See generally* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007) (assessing the impact of the Patriot Act amendments); Kris, *supra* note 31 (describing the impact of the new language on executive branch procedures).

[142] Mayfield v. United States, 504 F. Supp. 2d 1023, 1041-42 (D. Or. 2007).

[143] *Id.* at 1037.

[144] The *Mayfield* court's concern that a U.S. Person can be surveilled under FISA without probable cause to believe the target is guilty of a crime conflicts with how others read the pertinent provisons. One expert describes FISA as requiring a showing of suspected criminality before U.S. Persons may be targeted. *See, e.g.*, Kris, *supra* note 31, at 491 ("U.S. Persons can be agents of a foreign power only if they engage in some level of criminal activity.").

[145] The FISCR case was the first decided by that court. The FISCR reviewed the FISC's determination that the executive's procedures violated the Constitution. *In re* Sealed Case, 310 F.3d 717, 717 (Foreign Int. Surv. Ct. Rev. 2002) . In *Mayfield*, the target of allegedly unlawful surveillance brought a facial Fourth Amendment challenge to the government's surveillance of him, which the court granted despite the

In practice, the Fourth Amendment may constrain the executive branch's exiling decisions in ways that are not enforced and for which the victims receive no remedy. For example, to the extent that no one who is willing or able to challenge it learns of executive branch surveillance that violates the Fourth Amendment, that transgression will go unremedied. When Congress or the courts deny a court's power to review past transgressions, those transgressions escape punishment.

It seems clear that, in recent years, the executive branch has violated the Fourth Amendment rights of U.S. Persons by improperly exiling them — or depriving them of their full Fourth Amendment rights of judicial review. There has been reporting of extensive surveillance of the communications of U.S. Persons not suspected of being foreign agents as part of an extensive Terrorist Surveillance Program ("TSP") instituted in the wake of the September 11th attacks.[146] Plaintiffs, and their expert witnesses, have charged that the communications of U.S. Persons with foreign ties, if any, that are insufficient under the Fourth Amendment to justify exile, were nonetheless swept up in an extensive surveillance effort conducted by the National Security Agency.[147] Because that program proceeded without prior judicial review, as required by the Wiretap Act and FISA, such surveillance appears to have violated the Fourth Amendment.[148]

Acts by both Congress and the courts have made it less likely that the victims' Fourth Amendment rights will be vindicated. First, the Sixth Circuit denied standing to a group of plaintiffs and held that they could not establish that they had

---

governments' efforts to claim that he lacked standing. *Mayfield*, 504 F. Supp. 2d at 1023. *See also supra note* 128 (describing hurdles to bringing challenges to FISA).

[146] *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008); Bamford, *supra* note 55; Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[147] *See* Complaint, Hepting v. AT & T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. 06-CV-00672).

[148] *See* Maclin, *supra* note 16, at 1293-326 (arguing that the *Keith* case establishes the unconstitutionality of the TSP).

been injured by the TSP because state secrets prevented them from amassing evidence about the program. [149] Under the state secrets privilege, the executive may keep some foreign affairs information out of court and away from the public, to protect its need for secrecy.[150] Secondly, in recent amendments to FISA, Congress agreed to dismiss pending and future cases that challenged the assistance provided by telecommunications companies to the NSA as part of the TSP.[151] As a result, the NSA's conduct as well as that of the intermediaries may never face judicial review, and any Fourth Amendment violations will go unpunished and unremedied. Finally, those same amendments also reduced the amount of oversight that the FISC will give to exiling decisions by permitting the executive branch to submit protocols for surveillance rather than individualized cases for consideration.[152] Critics fear that the amendments provide insufficient oversight of the executive branch and effectively authorize "dragnet surveillance" that will sweep up the communications of innocent people without justification.[153] Civil liberties groups have challenged the amendments' constitutionality.[154]

---

[149] ACLU v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007). The Sixth Circuit recognized state's secrets as a bar to plaintiffs' efforts to acquire information about their surveillance by the NSA and therefore denied plaintiffs standing to sue. *Id.* That decision reversed ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (finding challenged NSA surveillance to violate the First, Fourth, and Fifth Amendments and other constitutional and statutory provisions).

[150] *See, e.g.*, *Hepting*, 439 F. Supp. 2d 974 (discussing state secrets privilege). *But see In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109 (N.D. Cal. 2008) (holding that the FISA provisions for judicial access to foreign surveillance information preempt the states secrets privilege, which is a creature of federal common law).

[151] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 110-261, §30, 122 Stat. 2436, 2468 (amended 2008).

[152] *See id.* at 2437-67.

[153] *See, e.g.*, Press Release, ACLU, Senate Passes Unconstitutional Spying Bill and Grants Sweeping Immunity to Phone Companies (July 9, 2008), *available at* http://www.aclu.org/safefree/general/35928prs20080709.html.

[154] *See, e.g.*, Complaint, Amnesty Int'l USA v. McConnell, No. 08 cv 06259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf; Motion to Dismiss, *In re* Nat'l Sec. Agency Telecomms. Records Litig., No. 06-1791 VRW (N.D. Cal. Oct. 17, 2008), *available at* http://www.eff.org/files/filenode/att/immunityoppocorrected.pdf (challenging constitutionality of grant of immunity to telecommunications company in the FISA

That executive branch agents may deprive people of their constitutional rights and face no repercussions is clearly a problem. Yet the controversy generated by these cases will likely yield some important reforms. For example, the FISA Amendments provide for review of the TSP and a report to Congress.[155] Litigation over the telecommunications company's involvement in the TSP has already generated important precedents about the appropriate use of the state secrets privilege.[156] All of these cases, and particularly the scandals, focus the public on the need for meaningful and sufficient judicial review of the executive branch's exiling decisions and of its use of "foreignness" to justify its surveillance, whether or not the facts support that characterization.

CONCLUSION

By generalizing about a complex area of law, one may view the rules pertaining to electronic surveillance as maintaining a virtual border between members of the national community who benefit from the protections of the Fourth Amendment and foreigners who do not. Benefits of full Fourth Amendment protections include the rigorous judicial review enunciated in *Berger* and codified in the Wiretap Act. Under those requirements, a judge conducts substantial oversight of executive branch surveillance before, during and after an investigation. Because of the inability of purely physical borders to separate those protected by the procedural requirements from those not so protected, electronic surveillance law determines when foreign persons acquire Fourth Amendment protections and when U.S. Persons lose them. The laws are designed to ensure that U.S. Persons will not be found to sacrifice the full protections of the Fourth Amendment until the government has established to a special court that the targeted person is an

---

Amendments Act).

[155] *See* FISA Amendments Act § 802.

[156] *See, e.g.*, Hepting v. AT & T Corp., 439 F. Supp. 2d 974, 992-94 (N.D. Cal. 2006) (denying government's claim that the states secrets privilege categorically barred an action accusing the defendant of violating plaintiffs' constitutional and statutory rights by assisting the NSA in the TSP).

agent of a foreign power based on more than just First Amendment protected activities. To the extent the laws permit the executive to exile without sufficient justification, oversight, and accountability, they should be fixed.

ESSAY

BORDER FICTION: DOES AN ANALOGY TO IMMIGRATION LAW ALLEVIATE FOURTH AMENDMENT ANXIETY?

Matthew R. Hall[*]

Does immigration law help resolve the Fourth Amendment problems posed by the movement of electronic information across the United States border? The answer, at least according to this Essay, is a conditional "yes." The lens of immigration law helps to clarify the idea that the border consists of a real physical line accompanied by a series of legal fictions. Understanding the ways in which immigration law has grappled with these legal fictions eases at least some of the difficulty confronting analysis of the Fourth Amendment "border doctrine" as it applies to the movement of digital data across the country's international border.

More specifically, this Essay explores several phenomena in immigration law and then draws an analogy between the resolution of those problems in immigration jurisprudence and potential resolutions under the border doctrine.[1] First, the

---

[*] Associate Professor, The University of Mississippi School of Law. The author received research and symposium participation funding from the National Center for Justice and Rule of Law at The University of Mississippi School of Law—the Center is funded by the Office of Justice Programs at the Department of Justice. The opinions expressed in this Essay, however, are those of Professor Hall alone.

[1] The Essay proceeds with the knowledge that the search for consistency through

Essay probes the division of immigration border crossings into a two-part typology and concludes that this typology could contribute to solving two problems under the border doctrine: the treatment of intranational electronic communications that incidentally cross the border and the question of when certain border searches constitute routine inspections rather than invasive intrusions. Next, the Essay examines the location of the border under immigration law, concluding that immigration's border rules apply not just at the physical border but also wherever the authorities locate an alien who recently entered the country without legal permission. This concept could aide in analyzing the appropriateness of applying the border doctrine to electronic information that enters the country without a moment for inspection paralleling the entry of letters or packages. Third, the Essay briefly touches on the extent to which immigration law builds on assumptions about the mental state of individuals who cross the border. Although a mental state analogy assists the border doctrine with regard to intranational communications that incidentally cross the border, it potentially impedes clear application of the border doctrine to many electronic communications when the parties have no knowledge of each other's physical location. Penultimately, the Essay then touches on the possibility that as with immigration enforcement, the federal government might consider the delegation of border doctrine responsibilities to state and local officials. The Essay concludes with the contention that border doctrine analysis would benefit from an explicit consideration of costs and benefits. Immigration law centrally considers cost-benefit analysis as part of the test for minimum constitutional due process. Although the Supreme Court has engaged in cost-benefit reasoning in criminal procedure cases, the jurisprudence of the border doctrine should explicitly recognize its importance

---

analogy does not necessarily lead to a just or wise result. *Cf.* Bankers Life and Cas. v. United States, 142 F.3d 973, 982 (7th Cir. 1998) ("While we do not doubt that 'foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines,' Ralph Waldo Emerson, *Self Reliance*, Essays: First Series (1841), we hope that our emphasis on consistency does not qualify as foolishness. On the contrary, consistency in the law forms the backbone of effective jurisprudence.").

in order to ensure consideration of the effects of suspicionless searches on a large scale.

Throughout, this Essay assumes familiarity with the Fourth Amendment's border doctrine and does not purport to offer a summary or detailed analysis of its principles.[2] Further, this Essay makes several assumptions about border doctrine analysis as it applies to electronic information. First, the Essay presumes that the transmission of electronic information through third-party conduits does not obviate the need for Fourth Amendment analysis.[3] Second, the Essay further assumes that the electronic information in question is not covered by free speech principles.[4] In other words, the Essay is predicated on the idea that government authorities would search an electronic communication not for its expressive content so much as for contraband or other illicit content, such as digitized images of child pornography or stolen classified information.[5] Finally, an important caveat: I offer this Essay as an exercise in brain storming the ways in which an analogy with established immigration law could help understanding of issues arising under the border doctrine. I am not comfortable with the extent to which immigration law provides aliens with few constitutional rights, nor do I believe that the border doctrine

---

[2] For full coverage of the border doctrine, see generally THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 399-463 (Carolina Academic Press 2008).

[3] *See* Smith v. Maryland, 442 U.S. 735, 742, 744-45 (1979) (holding that, by conveying a dialed phone number to the telephone company, a claimant "assumed the risk that the company would reveal to police the numbers he dialed"); United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148 (C.D. Cal. 2007) (finding, in a civil case under the Wiretap Act, that the defendant did not intercept emails but instead obtained them from electronic storage).

[4] *See* United States v. Ramsey, 431 U.S. 606, 623-24 & n.18 (1977) (holding that the search of a letter for contraband, with regulatory protection of the contents, did not raise First Amendment concern).

[5] With the child pornography serving as the equivalent of the heroin at issue in *Ramsey*. *See id.*

accords United States citizens sufficient protection. This Essay does not attempt to deploy a critique of either body of jurisprudence, nor does it suggest whether the remedy lies in the reformulation of constitutional law or in statutory protections.

THE LEGAL FICTION OF THE BORDER

As a starting point, consider the concept of the border under immigration law. As a geopolitical boundary giving shape to the United States, the immigration border plays an essential role in defining the nation—the people. Fundamentally, immigration law governs the movement of people across the border. Nevertheless, in terms of jurisprudence, immigration law engages in a dramatically aggressive legal fiction regarding the border.

Imagine an alien arriving, for the first time, in the United States via airplane at Boston's Logan Airport. Conventional wisdom would hold that as the plane touches the tarmac the alien has landed on United States soil.[6] Yet, under immigration law, no such legal transition takes place. Immigration law treats a newly-arriving alien, even one standing on our soil at the airport, as standing just on the other side of our border awaiting permission to step over.[7] The implications of this legal fiction profoundly affect the alien's legal status. Despite an arriving alien's physical presence within our territory, immigration jurisprudence dictates that the individual's rights

---

[6] One might even expect that the transition into United States territory occurs as the plane enters the country's airspace.

[7] *See* 8 U.S.C. § 1225(a)(1) (2006) ("An alien present in the United States who has not been admitted or who arrives in the United States (whether or not at a designated port of arrival and including an alien who is brought to the United States after having been interdicted in international or United States waters) shall be deemed for purposes of this chapter an applicant for admission."); *see also* United States *ex rel.* Knauff v. Shaughnessy, 338 U.S. 537, 542 (1950) ("At the outset we wish to point out that an alien who seeks admission to this country may not do so under any claim of right. Admission of aliens to the United States is a privilege granted by the sovereign United States Government. Such privilege is granted to an alien only upon such terms as the United States shall prescribe. It must be exercised in accordance with the procedure which the United States provides.").

differ very little from someone requesting a visa at one of our consulates overseas.[8] Most significantly, a newly-arriving alien possesses no due process rights.[9] Upon a determination that the alien does not qualify for entry into the United States, regardless of whether the alien obtained a visa ahead of time, the immigration authorities could send the alien home immediately with no legal recourse and certainly no hearing.[10] In contrast, a returning lawful permanent resident, even one found inadmissible by the immigration authorities at the border, would receive a full deportation hearing (or in the language of the immigration statutes, a "removal" hearing) and would enjoy the right to seek review in federal court.[11]

Why the stark contrast? In a nutshell, under immigration law, a newly-arriving alien does not constitute a "person" under the Fifth Amendment's Due Process Clause.[12] For purposes of

---

[8] Many cases explain the consular non-reviewability doctrine. *See, e.g.*, United States *ex rel.* Ulrich v. Kellogg, 30 F.2d 984, 986 (D.C. Cir. 1929); United States *ex rel.* London v. Phelps, 22 F.2d 288, 290 (2d Cir. 1927); Li Hing of Hong Kong, Inc. v. Levin, 800 F.2d 970, 970-71 (9th Cir. 1986); Ventura-Escamilla v. INS, 647 F.2d 28, 30-31 (9th Cir. 1981); Garcia v. Baker, 765 F. Supp. 426, 428 (N.D. Ill. 1990).

[9] *See* Adam B. Cox. & Eric A. Posner, *The Second-Order Structure of Immigration Law*, 59 STAN. L. REV. 809, 822 (2007) ("Courts have at times suggested that the government may exclude such a noncitizen for any reason—even on the basis of race or some other ground that would ordinarily be constitutionally suspect. Similarly, courts have sometimes intimated that the government is free to enforce its exclusion policy with whatever summary procedures it deems appropriate, on the ground that the Due Process Clause does not constrain the government in such situations." (footnote omitted)); *but see id.* at 822 n.63 (questioning whether courts have understated the rights of arriving aliens).

[10] *See* 8 U.S.C. § 1225(b)(1)(A) (2006) ("If an immigration officer determines that an alien . . . who is arriving in the United States . . . is inadmissible . . . the officer shall order the alien removed from the United States without further hearing or review unless the alien indicates either an intention to apply for asylum . . . or a fear of persecution."); 8 C.F.R. § 235.3(b) (2008).

[11] *See* 8 U.S.C. § 1225(b)(2) (2006); Cox & Posner, *supra* note 8, at 822 ("The government is more constrained by the Constitution when it takes an immigration-related action against a noncitizen who has achieved a greater constitutional status than a first-time arriving alien. Courts suggest that noncitizens may receive additional constitutional protections when they have entered the territory of the United States, when they have established significant ties to the United States, or when they have achieved a legal immigration status under statutory and regulatory immigration law.").

[12] *See* Shaughnessy v. United States *ex rel.* Mezei, 345 U.S. 206, 212 (1953) ("It is true that aliens who have once passed through our gates, even illegally, may be expelled

the application of constitutional due process rights at the immigration border, only a United States citizen or an alien with pre-existing ties to the country constitutes a person.[13] Thus, immigration law takes an extraordinarily legalistic, rather than realistic, view of the border even when the issue at hand concerns the most fundamental question of who amounts to a human-being deserving of full legal cognition. The immigration border is not a physical demarcation, but instead an abstract legal construct.

In distinction, because Fourth Amendment jurisprudence deals primarily with events inside the United States and with individuals fully entitled to constitutional protection, the border receives starkly different treatment. Courts tend to view the border as a physical line and accordingly apply Fourth Amendment border doctrines only at or in proximity to that physical border.[14] Because the vast majority of Fourth Amendment cases arise in contexts where the normal rules of reasonable suspicion or probable cause apply to searches and seizures, Fourth Amendment jurisprudence treats the border doctrine with suspicion, only reluctantly suspending those traditional protections against governmental intrusion.[15]

If there is a lesson to learn from immigration law on this front, it lies in the idea that the Constitution operates differently at the border. Phrased differently, immigration law

---

only after proceedings conforming to traditional standards of fairness encompassed in due process of law. But an alien on the threshold of initial entry stands on a different footing: 'Whatever the procedure authorized by Congress is, it is due process as far as an alien denied entry is concerned.'") (internal citations omitted).

[13] *See id.* Indeed, under immigration law, this concept is not only unsurprising, it is closer to the norm than the exception. The vast majority of people in the world—including the many who wish to come legally or illegally to the United States—fall outside the protections of the Constitution. *See generally* Note, *The Extraterrial Constitution and the Interpretive Relevance of International Law*, 121 HARV. L. REV. 1908 (2008).

[14] Some cases extend the border to its functional equivalent—airports or package sorting centers. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 272-73 (1973); United States v. Abbouchi, 502 F.3d 850, 854 (9th Cir. 2007).

[15] For instance, scholars refer to the "border search exception." *See* Larry Cunningham, *The Border Search Exception as Applied to Exit and Export Searches: A Global Conceptualization*, 26 QUINNIPIAC L. REV. 1 (2007).

teaches that the border is not a locus for constitutional exceptionalism, but instead the constitution applies uniquely at the border and in a manner that entails the application of legal fiction rather than realism.

THE IMMIGRATION TYPOLOGY

Turning from grand theory to more mundane matters, immigration law presents a two-part typology of border crossings that might aid in the analysis of Fourth Amendment concerns at the digital border. First, immigration law distinguishes between what we might call "incidental" border crossings and "genuine" border crossings. Secondly, immigration law treats border crossing differently depending upon whether the individual seeking entry is a citizen, a resident alien, or a newly-arriving alien.

An incidental border crossing occurs, for instance, when a flight leaves Los Angeles International Airport and lands at Honolulu International Airport. Factually, all the passengers departed from and reentered into the territory of the United States. Nevertheless, for immigration purposes, no border crossing occurred, and no one on the flights need demonstrate their admissibility into the country.[16] The presence of the passengers outside the United States took place only incidentally to their transport from one point in the territory of the country to another. In contrast, a genuine border crossing occurs whenever people seek to enter the United States from a point outside—a point from which they had access to a foreign or international territory.

Further, as alluded to previously, immigration doctrine prescribes different levels of process for different categories of entrants into the United States. A United States citizen, who demonstrates citizenship at the border,[17] could return to the country, and presumably could challenge any immigration proceeding immediately in federal court, asserting that the

---

[16] *Cf.* 8 U.S.C. § 1221(a) (2006) (mandating an arrival manifest for arriving passengers only for flights from outside the United States).

[17] *See* 8 C.F.R. § 235.1(b) (2008).

immigration authorities lacked jurisdiction.[18] A resident alien (a lawful permanent resident, an asylee, or a long-term visitor) seeking to reenter the country would normally receive admission but upon a finding of inadmissibility, would face a removal hearing. In distinction, a newly-arriving alien, upon a finding of inadmissibility, would face expedited removal proceedings and would not receive a hearing.

The first step in the immigration typology might help resolve the Fourth Amendment dilemma of whether intranational digital communications (which travel from inside the United States to inside the United States and happen to cross the boundaries of the country due to the vagaries of electronic communications technology) fall under the ambit of the special search and seizure rules of the Fourth Amendment border doctrine.[19] Accordingly, an intranational phone call bounced off a satellite, or a similar email routed through a switch in Europe, both constitute the equivalent of "incidental" border crossings. Immigration law suggests that no particular border doctrine should apply. Where Fourth Amendment analysis might consider whether such communications constitute an exception to the border doctrine, which itself represents an exception to the normal Fourth Amendment rules, immigration law treats this pattern seamlessly and fluidly, rather than conceptualizing of it as an exception to an exception. Under immigration law, an incidental border crossing does not entail a request for admission into the United States. By

---

[18] *See* 8 C.F.R. § 235.3(b)(5)(iv) (2008) (detailing the treatment of claims of United States citizenship); *cf.* 8 U.S.C. § 1101(a)(3) (2006) (defining "alien" as a person not a citizen of the United States).

[19] As Professor Tom Clancy notes:

> On the other hand, in today's world, the most routine in-state phone call may be routed to a satellite; an email to someone in the United States from someone in the United States may pass anywhere over the Internet. Are such communications now permissibly examined as border searches? One possible solution to such a quandary is to find the border search doctrine inapplicable, based on the wholly intra-national nature of the origin and destination of the communication, ignoring the technical means by which the communication is achieved. This functional approach satisfies the sovereignty concerns underlying the border search doctrine.

CLANCY, *supra* note 2, at 412.

analogy, an intranational electronic communication that incidentally crosses the border does not trigger the border doctrine.

The second step in the immigration typology could assist courts in analyzing the propriety of examining digitized information on laptop computers carried by international passengers.[20] To the extent courts continue to analyze such searches to determine whether they constitute routine exams (permissible without any particularized suspicion) or non-routine and invasive (requiring suspicion adequate to justify the intrusion), the immigration typology militates in favor of giving prominent consideration to the owner's status—citizen, resident alien, or arriving alien. In broad terms, and absent other considerations,[21] an analogy to immigration law might lead to the following doctrine: (1) border officials may search an arriving alien's laptop with no suspicion, (2) border officials may search a resident alien's laptop only with suspicion, and with the balance struck in favor of allowing a very invasive search based only on minimal suspicion, and (3) border officials may search a citizen's laptop only with suspicion, and with the balance struck in favor of allowing a particularly invasive search based only on heightened suspicion. Alternately, and perhaps more simply, the immigration analogy dictates that arriving aliens face searches of their laptops routinely, resident aliens face such searches on a semi-routine basis, and citizens face searches on non-routine grounds.

Perhaps, the analogy to the immigration typology can stretch even farther to cover international electronic communications generally. One might divide international electronic communications between those communications that originate in the United States and those that originate abroad.

---

[20] For the debate over laptop computers, see *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); and the significant body of law review commentary already surrounding these cases.

[21] This analysis does not purport to delve into the First Amendment implications of border officials examining the expressive content of digital information contained on the laptop. Perhaps it makes the most sense to conceive of the border officials as searching for contraband data such as images of child pornography.

Conceivably, communications originating in the United States analogize to citizens or resident aliens, while those originating abroad analogize to arriving aliens. Searches of the former should require reasonable suspicion, while the Fourth Amendment border doctrine should allow suspicionless searches of the latter. This effort ultimately breaks down and becomes facile because so many electronic communications will entail dialog such that surveillance of one end of the exchange inevitably trenches on the other end as well. Similarly, a significant number of exchanges will entail communication with a United States citizen or resident alien abroad and a counterpart here in the country, rendering the analogy strained at best.

THE LOCUS OF THE BORDER

Another aspect of immigration jurisprudence that illuminates Fourth Amendment issues regarding digital information arises upon consideration of the treatment of aliens who enter the United States illegally, without admission at the border. These aliens, despite their presence inside the United States, remain for up to two years in the same status as newly-arriving aliens: they face removal without hearing.[22] As such, the immigration border constitutes not only a physical border at the nation's boundary, but a continuing legal status attaching wherever the government locates an unadmitted alien within the United States. Understood differently, immigration border rules apply not just at the time a person crosses the physical border; the border rules also alter the status of any person who fails to legally cross the physical border. Aliens illegally in the United States continue under the legal fiction of standing at the border seeking admission. One might go so far as to say that immigration law views the border having a legal locus attached to a person, rather than only to the physical line demarcating the boundary of the United States. While the physical border is porous, the legal border remains consistent.

How does this immigration concept relate to digital

[22] *See* 8 U.S.C. § 1225(b)(1)(A) (2006); 8 C.F.R. § 235.3(b) (2008).

information? The Fourth Amendment border doctrine applies to things and people as they cross the border. Electronic information simply does not cross the border in the same tidy manner. It enters the United States both from space via satellite and, even when it enters via a land line, it may move virtually immediately to its destination inside the country without pausing at a shipping or distribution hub as it crosses the physical border. Even if electronic information presented no other unusual concerns, this fact alone would render application of the border doctrine difficult. A vast quantity of electronic information enters the United States without an opportunity for inspection, paralleling the treatment of people and things at the physical border.

Although immigration law provides an imperfect analogy, it certainly offers guidance. The Fourth Amendment could treat digital information that enters the United States without opportunity for inspection in the same manner as immigration law treats unadmitted aliens inside the country. In a legal fiction, that information would remain for a reasonable length of time metaphorically standing at the border awaiting inspection. This proposed rule is not without significant complication. The vast majority of people legally in the United States possess identification that facilitates an efficient screening for immigration purposes. Information does not authenticate itself so readily—for example, a domestic child pornography digital image file could closely resemble a foreign file. Further, the prospect of allowing suspicionless searches, under the border doctrine, of digital information in the hands of people within the United States poses considerable civil liberties concern.

The proposal of treating digital information that enters the United States without a formal border crossing in the same manner as an unadmitted alien also has some potential for helping to resolve a perplexing difference between physical international communication via letters and packages, on the one hand, and electronic communications, on the other hand. With physical communication, the border crossing occurs at the initiation of the sender, and it takes place in short order thereafter, through the relatively centralized channels of

shipping and sorting facilities. With electronic communication, the border crossing may likely occur at the initiation of the recipient and may take place long after the sender has acted. Further, electronic communications more typically travel through the relatively decentralized channels of the internet. With email (assuming inaccurately that the message travels as one piece of data)[23] the communication would travel from the sender to the recipient's email server (a trip that might entail one or more border crossings) and then to the recipient's computer (another trip that might entail one or more border crossings). Although electronic surveillance technology may permit monitoring of the communication as it crosses a border at either of these stages, it may also be the case that the government cannot examine the message until it takes up residence (or is viewed) inside the United States. By focusing on the "unadmitted" electronic communication, rather than the moment that data literally entered the country, the border doctrine could prevent the particularities of electronic communications technology from vitiating the government's prerogative to conduct searches of all that crosses the border.

IMMIGRATION MENTAL STATE

Consideration of the role of mental state in immigration border crossings may also illuminate the problems inherent in the application of the border doctrine to electronic communications. Morally, immigration law works, at least in part, because very few people cross the border unintentionally or in ignorance of the legal significance of such activity. Aliens seeking entry generally understand they need a visa, aliens legally within the United States know they need a reentry permit, and United States citizens generally understand they need a passport. Under immigration law, movement across the border without proper documentation subjects one to immigration consequences—knowledge and settled expectations

---

[23] *See* John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 261 (2008) ("Any communications of any significant size are divided into separate packets for travel across the network").

undergird the legal regime.[24]

Perhaps a similar pattern pertains in the realm of the Fourth Amendment. Although the Supreme Court seems to predicate the border doctrine primarily on sovereignty, the reasonableness of the rule also appears to lie in notions of volition. Presumably, those who present themselves or their property at the border expect some level of examination, and we could even understand them to implicitly consent to search. If this line of reasoning holds true, the previous analogy between intranational communications that incidentally cross the border and intranational travel that incidentally crosses the border gains strength. Part of the underlying logic for treating the two cases similarly arises from the intent of the participant—to the extent the individual possesses any intent to cross the border or send data across the border, it exists only for the purpose of completing the intranational act. Accordingly, the individual lacks the mental state necessary to reach a conclusion of implied consent for a border search.

The mental state rationale, however, makes analysis of electronic communications more difficult. We can discern the intent to cross a border from the address on international packages or letters; no such inference readily arises with email or internet communications because the parties may not know each other's physical location.[25] Because this mental state arises only as a speculative accessory to the Supreme Court's actual justification for the border doctrine, it should not defeat the application of the rule to electronic communications.

DELEGATION TO STATE AND LOCAL LAW ENFORCEMENT

Immigration law presents an unusual model for joint federal, state, and local enforcement that may offer some promise for the Fourth Amendment border doctrine as it applies

---

[24] *Cf.* 8 U.S.C. § 1326 (2006) (prescribing criminal penalties for aliens who enter the United States after denial of admission or who reenter the United States after removal).

[25] With the increasing use of mobile phones, the same logic holds increasingly true for phone communications as well.

to electronic information.[26] Under contemporary immigration law and jurisprudence, the immigration power constitutes a virtually exclusive federal province.[27] Nevertheless, state and local governments have long possessed the authority to enforce criminal immigration laws and have recently received increased power to participate in civil immigration enforcement.[28] The Supreme Court has repeatedly stated that the immigration power, like the border doctrine, constitutes a plenary power in the hands of the federal government, arising directly out of national sovereignty itself.[29]

Accordingly, given the similar status of the two powers, it might be possible for the federal government to share the border doctrine power with state or local law enforcement. This notion may take on particular vigor as legal focus shifts from the traditional physical border to the electronic border. The physical border presents relatively few ports of entry for letters and packages—the nation's international air and seaports mainly. While, of course, these ports of entry lie within states, their small number makes federal customs and immigration enforcement practicable. The electronic border knows no such limitations. Rather than consisting of the nation's boundaries plus airports, the electronic border would more properly be

---

[26] For coverage of the debate over state and local enforcement of civil immigration laws, see generally Clare Huntington, *The Constitutional Dimension of Immigration Federalism*, 61 VAND. L. REV. 787 (2008); Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137 (2008); Cristina M. Rodriguez, *The Significance of the Local in Immigration Regulation*, 106 MICH. L. REV. 567 (2008); Michael J. Wishnie, *State and Local Police Enforcement of Immigration Laws*, 6 U. PA. J. CONST. L. 1084 (2003); and LISA M. SEGHETTI, STEPHEN R. VIÑA & KARMA ESTER, CONG. RESEARCH SERV., ENFORCING IMMIGRATION LAW: THE ROLE OF STATE AND LOCAL LAW ENFORCEMENT (2005), http://www.au.af.mil/au/awc/awcgate/crs/rl32270.pdf.

[27] *See* DeCanas v. Bica, 424 U.S. 351, 354 (1976); Hampton v. Mow Sun Wong, 426 U.S. 88, 101 n.21 (1976).

[28] *See, e.g.*, Seghetti et al., *supra* note 26, at 6-22.

[29] *Compare* United States v. Ramsey, 431 U.S. 606, 616 (1977) (acknowledging the plenary power of customs officials), *and* United States v. Montoya de Hernandez, 473 U.S. 531, 537-39, 544 (1985) (likening customs officials conducting border searches to immigration officials), *with* Shaughnessy v. United States *ex rel.* Mezei, 345 U.S. 206, 210 (1953) (describing the long tradition of according plenary power over immigration to Congress and the Executive).

conceived of as consisting of all telecommunications networks—including satellites. Thus, the exponential growth of the border as it makes the transition from physical to electronic may overwhelm the capacity of the federal government to conduct adequate screening efforts. Similarly, as explained above, the prevalence of electronic information that, like an illegal alien, has not formally crossed a border may also outstrip the resources of the federal government. A partnership between federal authorities and state and local officials could conceivably ameliorate this problem.[30]

Cost / Benefit Analysis

Although immigration jurisprudence accords aliens with few constitutional liberties, the Fifth Amendment's Due Process Clause does provide some solace, at least for aliens legally admitted to the United States.[31] Indeed, an analogy with due process analysis represents the greatest benefit that immigration law has to offer the Fourth Amendment's border doctrine. Under the seminal *Mathews v. Eldridge* test, courts weighing whether or not a particular procedure accords a litigant constitutionally adequate process consider three factors: (1) the private interest at stake, (2) the risk of error under current procedures and the reduction of risk possible with additional procedures, and (3) the costs and lost efficiencies of implementing additional procedures.[32] Essentially, this test directs the court to consider the costs and benefits of procedures. Moreover, cost-benefit analysis directs the court to look beyond the case at hand and examine the effects of the rule on other cases—or at least other iterations of the same. The test looks toward statistical considerations (risk and reduction of risk) and toward the effects of repetitive application (cost and lost efficiency).

---

[30] Of course, such a partnership could also raise concerns paralleling those arising from proposed partnerships for civil immigration enforcement.

[31] *See* Landon v. Plasencia, 459 U.S. 21, 34-35 (1982) (applying the standard due process to immigration proceedings).

[32] Mathews v. Eldridge, 424 U.S. 319, 334-35 (1976).

Why does cost-benefit analysis hold promise for border doctrine cases? Fundamentally, border doctrine searches, because they occur without particularized suspicion, affect an enormous number of individuals for each case that nets the government criminal conduct.[33] Yet, if the cases most actively litigated arise out of those "hits" rather than out of the "misses," a danger arises. The search program superficially appears successful after the fact of a positive result—it appears justified because it succeeded. Inversely, the search program appears questionable if it rarely or never finds criminal conduct. Because the cases in which criminal conduct comes to light receive more attention, they tend to skew perception of the statistical reality. This is the investigator's version of the "prosecutor's fallacy"[34] —the logical problem of believing that you have used a good investigatory process because you have caught a criminal.

By explicitly deploying cost-benefit analysis as part of the reasonableness inquiry into the validity of a border doctrine search program, the courts would ensure consideration of the statistical reality of the program, and its effects on innocent parties, rather than risk the possibility of improper focus on the potentially misleading success of the program. Indeed, the Supreme Court has repeatedly stated, in suspicionless search cases, that empirical evidence regarding the statistical success

---

[33] One could refer to suspicionless searches, like those conducted under the border doctrine, as "stochastic" searches. They take their logic not from particularized suspicion underlying each search, but from the assertion that statistically they will catch criminal conduct. The problem with such an assertion is that, statistically, any programmatic search or surveillance of the public will catch some number of criminals.

[34] The classic version of the prosecutor's fallacy arises if genetic testing reveals that only one in 100,000 people have the same DNA as the suspect and the perpetrator. This information appears incriminating. But, if the events occur in a city of 1,000,000 people, then nine innocent people have DNA that matches the perpetrator. This information appears powerfully exculpating. In the case of the border doctrine, the ex post phenomena of litigating the case of the apparently guilty creates a similar false impression regarding the effectiveness of the screening procedures at the border. If we learn that only one out of every 100,000 searches results in a positive, we might not feel the same confidence in the process ex ante that we enjoy during the prosecution of the one success.

of the search program matters.[35] The Court has stopped short of mandating evidence that the program contributes to law enforcement and that it produces some reasonable number of hits, but has instead struck down one program, in part, because it lacked such evidence and upheld another, in part, because it possessed this kind of evidentiary support.[36] Border doctrine jurisprudence would benefit enormously if the Court explicitly recognized its practice of examining empirical evidence in the special needs cases and applied similar reasoning to border doctrine cases by demanding either empirical evidence or, at least, a cost-benefit analysis. It seems a Catch-22 to require empirical evidence of a reasonable program that may not yet have an established track record; but even a proposed program will have potential costs and benefits.

Critics may contend, with significant force, that cost-benefit analysis will erode civil liberties by focusing a court unduly on law enforcement (or national security) benefits and allowing those interests to outweigh one individual's rights. While this criticism may prove accurate, this Essay operates on the intuition that current analysis of border doctrine cases skews in the opposite direction—it tends to minimize the intrusion on many innocents because a seemingly guilty party appears before the court. A court conducting cost-benefit analysis, by necessity, will consider not just the litigant snared by the border search, but all those innocents upon whose interests the government intruded. In other words, this Essay takes the position that cost-benefit analysis—by directing courts to consider the effect of programmatic search programs on the innocent—will result in

---

[35] *See* Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 454-55 (1990); Delaware v. Prouse, 440 U.S. 648, 659-63 (1979).

[36] *Cf.* Lawrence Rosenthal, *The Crime Drop and the Fourth Amendment: Toward an Empirical Jurisprudence of Search and Seizure*, 29 N.Y.U. REV. L. & SOC. CHANGE 641, 680 (2005) ("[S]urely we should at least consider the rate at which a given investigative practice has disclosed criminal activity when assessing its constitutionality. The Fourth Amendment proscribes 'unreasonable' searches and seizures; that would seemingly make empirical evidence of the efficacy of a challenged practice highly relevant. Evidence that a challenged practice pays important law enforcement dividends seems no less important. Yet it is striking that the Supreme Court—with only rare exceptions like *Martinez-Fuerte* and *Sitz*—neither looks at nor insists on empirical evidence.").

the aggregation of individual rights and the weighing of that aggregate interest (rather than a single guilty individual's interest) against society's law enforcement agenda.

CONCLUSION

Immigration law and jurisprudence may offer some significant assistance in resolving particular dilemmas arising with the application of the border search doctrine to the movement of electronic information. The most important contribution, however, would come if courts considering the reasonableness of programmatic, or statistical, searches—such as the vast majority of the suspicionless searches conducted at the border—performed some form of cost-benefit analysis as courts do when considering the constitutionality of immigration procedures under the constitutional guarantee of procedural due process.

COMBATING TERRORISM IN THE DIGITAL AGE: A CLASH OF DOCTRINES: THE FRONTIER OF SOVEREIGNTY—NATIONAL SECURITY AND CITIZENSHIP—THE FOURTH AMENDMENT—TECHNOLOGY AND SHIFTING LEGAL BORDERS

Harvey Rishikof[*]

> I guarantee you this: neither the drafters of the Fourth Amendment, nor the Supreme Court when it crafted the 'border search exception,' ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information. . . . If you asked most Americans whether the government has the right to look through their luggage for contraband when they are returning from an overseas trip, they would tell you yes, the government has that right. But if you asked them whether the government has a right to open their laptops, read their documents and e-mails, look at their photographs, and examine the websites they have visited, all without any suspicion of wrongdoing, I think those same Americans would say that the government absolutely has no right to do that. . . . Ideally, Fourth Amendment jurisprudence would evolve to protect Americans' privacy in this once unfathomable situation. But if the courts can't offer that

[*] Professor of Law, former Chair, Department of National Security Strategy, National War College. The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, or the U.S. government.

> protection, then that responsibility falls to Congress.[1]
>
> Senator Russ Feingold 2008

> The threat of catastrophic attack with nuclear weapons has the greatest potential impact on our way of life and in terms of human cost.[2]
>
> A 2006 poll of 116 terrorism specialists representing a cross-section of political perspectives placed the likelihood of "a terrorist attack on the scale of 9/11 occurring in the United States" in the next five years (by the end of 2011) at 79 percent.[3]
>
> We are on borrowed time.[4]
>
> James E. Baker
> *In the Common Defense*

In a pre-9/11 conversation with a United States Supreme Court Justice he/she casually noted to me that when thinking about the different challenges for the law, "we are more or less settled in the Fourth Amendment area" and that the more interesting jurisprudence would be taking place elsewhere. This was a view held by many in the judicial world; however, this consensus has proven to be a premature assessment of the Fourth Amendment and the role of the Supreme Court.

Those who maintained this position underestimated the relationship of critical trends in the marketplace, the nature of modern threats to the state, theories of sovereignty and how the

---

[1] *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. (June 25, 2008) (statement of Sen. Russ Feingold, Chairman, Subcomm. on the Constitution of the S. Comm. on the Judiciary), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3420&wit_id=4083 (last visited Nov. 28, 2008).

[2] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 307 (Cambridge Univ. Press) (2007).

[3] *Id.* at 242.

[4] *Id.* at 6.

modern state has begun to approach the concept of privacy when it comes to borders. In fact, these new threats to the state, given the context of the law, have made "border security" and our understanding of the Fourth Amendment, an intellectual pivot point for our expectation of privacy in the 21st century. The state, in the face of a rapidly changing world of technology and while pursuing its fundamental prerogative to defend the nation, has taken a theoretical position, supported by the Supreme Court, that is transforming our very notion of citizenship.

In order to present my argument it is necessary to begin with a set of interlocking propositions that concern the evolving market place in the digital age of communication, the nature of modern threats to the state, the authority of the state to defend itself and the current threads of Supreme Court constitutional analysis in the Fourth Amendment arena. This paper will conclude with a discussion of how these interlocking propositions have created a clash of legal, political and social doctrines.

I. A Set Of Interlocking Propositions:

A. The Market Place: The Digital Age of Communications

The technological computer revolution is not reversible. The world of laptops, cell phones, PDAs, MP3 players and memory sticks has created an information revolution. This "portability" of property and expression has created an ability to generate a sea of information, transport the sea of information and then comment and create new seas of data. The full ramifications of this revolution are still being played out as a social force.[5]

---

[5] The concept of "ubiquitous technology" was explored in a law journal article by Susan Brenner where she noted that the physical and informational barriers historically used to differentiate between the public and private sectors of individuals' lives were being undermined by technology, and the Fourth Amendment would require "spatial" updating to remain viable. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 Miss. L. J. 1, 83 (2005).

The Internet has contributed by creating "pipes" and downlinks that allow interglobal communication from Shanghai to Washington in the blink of an eye. We all have become accustomed to the ability to communicate seamlessly at any time, from any place, with a variety of devices at our disposal.

It is believed that the next predicted revolution will take place in the soft "bio-technological" arena where billions of dollars are being invested to create products that will be able to store even greater banks of data on even smaller and more transportable devices. In fact, "chosen VIP clubbers" in Barcelona have been able to implant RFID chips in their arms that allow them to enter nightclubs with an electronic scan and pay for drinks with a similar scan.[6] The chip negates the need for identification cards or even money, since it acts as a debit card.[7] Given the technology, vast amounts of information could be similarly placed on a chip, implanted in an arm and then transported across the border. Where this type of technology will lead is limited only by the imagination.

These developments have contributed to the erosion of borders pertaining to the passage of information. The world of *hard copy* information remains only for the final act of reading; technology has already placed in the market the "electronic book tablet" that allows entire texts to be downloaded and electronically marked for underscoring and quoting.[8] This innovation potentially allows for downloading reading material at multiple access points. Moreover, as has been documented elsewhere, these technological changes have created a different

---

[6] Posting of Duncan Graham-Rowe to New Scientist news blog, *available at* http://www.newscientist.com/article.ns?id=dn5022 (May 21, 2004) (last visited Nov. 28, 2008) ("The chips are 1.2 millimetres wide and 12 millimetres long and look like a long grain of rice. A medically trained person injects the chip under the skin in the upper left arm, by the triceps. A scanner reads the chip by emitting a radio signal. This energizes the chip and causes it to send out a small radio frequency signal. This can be picked up from about 10 centimetres away.").

[7] *Id.*

[8] James Thompson, *The Big Question: Do electronic books threaten the future of traditional publishing?*, THE INDEPENDENT, July 24, 2008, *available at* http://www.independent.co.uk/life-style/gadgets-and-tech/features/the-big-question-do-electronic-books-threaten-the-future-of-traditional-publishing-875724.html (last visited Nov. 4, 2008).

approach to information and access for the next generation. The new generation of MySpace, Facebook and YouTube users are more open about information, share more easily and assume a reduced sphere of privacy.[9]

In short, the first proposition is that the digital information super highway is *omnipresent* and *omniaccessible* and *irreversible*. These developments have led some to question whether national borders are just speed bumps on the information super highway. How will or should the state and law respond to this proposition?

B. The Modern Threats: Individualized Privatized Weapons of Mass Destruction to Economic Espionage

The leitmotif for the twenty-first century is the increased "individualization" of the threat to the modern state. Niall Ferguson, in a book review provided that Phillip Bobbitt, the noted national security theorist, describes the terrorist threat as the intersection of "decentralized, privatized, outsourced and in some measure divorced from territorial sovereignty."[10] Individuals have access to a potential toxic cocktail of nuclear, biological, radiological and chemical weapons that can trigger mass destruction. A former special assistant to the President, legal adviser to the National Security Council, and now federal judge for the Court of Military Appeals, described "the threat of catastrophic attack with nuclear weapons" as having "the greatest potential impact on our way of life . . . in terms of

---

[9] Anthony Lilley, *Public is the new private for the MySpace generation*, THE GUARDIAN, March 23, 2006, at 8 of Media news and feature, *available at* http://www.guardian.co.uk/media/2006/mar/20/mondaymediasection.digitalmedia (last visited Nov. 28, 2008). Naturally, there is a movement to regain one's anonymity. One is the "de-tagging" phenomenon, whereby one tries to remove his or her name from a picture on Facebook; however, the picture continues to exist somewhere. *See* Lisa Gurensey, *Picture Your Name Here*, N.Y. TIMES at 6, July 27, 2008, *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html (last visited Nov. 28, 2008).

[10] Niall Ferguson, *War Plans*, N.Y. TIMES, April 13, 2009, *available at* http://www.nytimes.com/2008/04/13/books/review/Ferguson-t.html (last visited Dec. 2, 2008) (Terror and Consent book review). *See also* PHILIP BOBBITT, TERROR AND CONSENT (Alfred A. Knopf 2008).

human cost" and being a threat that is "perpetual, indefinite, endless, and not just long."[11] This is the widespread consensus among practitioners. "A 2006 poll of 116 terrorism specialists representing a cross-section of political perspectives placed the likelihood of a 'terrorist attack on the scale of 9/11 occurring in the United States' in the next five years (by the end of 2011) at 79 percent."[12]

What makes the threat so bedeviling is that it is not state based, per se. Since the Treaty of Westphalia in 1648, the unit of analysis for the international system has been the state. The advantage of the state being the source of a threat is that the sovereign is subject to deterrence. Following the Treaty, all sovereigns understood that they could be held responsible for any projections of force and that retribution might result in the personal loss of power and ultimately, subjugation of their people to a new, more powerful political entity. This "realist" perspective, based on the history of modern warfare, acted as a restraint on action until a state calculated whether it would be able to use force and not be disciplined or whether it would acquire enough force to begin a campaign of expansion and suffer the consequences if defeated. The advent of nuclear weapons has raised the stakes for this calculation since now the potential for total annihilation is a possible outcome of any reckless use of force. The modern era of mutually assured destruction between the superpowers produced at times an anxiety-ridden *Pax Americana*, but it achieved the ultimate goal of restraining nuclear use.[13]

This international system of nuclear restraint has been upset by the potential ability of a small group of fanatically dedicated individuals to acquire and explode a nuclear bomb. The technology, although far from simple, is not so difficult as to make it impossible. One merely needs the fissionable material, a triggering mechanism and a delivery system. When possessed by a state, deterrence has been the solution since a delivery

---

[11] BAKER, *supra* note 2, at 307, 309.

[12] BAKER, *supra* note 2, at 242.

[13] *See* HANS MORGENTHAU, POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE (Alfred A. Knopf) (4th ed. 1967).

system is usually associated with missile capacity.

The focus on missile capacity is unfortunately a failure of imagination. From the world of fiction, a former television journalist imagined one of the more creative solutions for a "delivery system."[14] In the novel *A Murder of Crows*, the Soviet Union, in an effort to undermine the United States nuclear "missile shield" and encourage disarmament, smuggles into the country sixty thermonuclear devices disguised as large industrial boilers.[15] The plan is to pre-position the "devices" in a number of major cities, thus neutering the missile shield and undercutting any potential for a preemptive first strike by the United States.

Although there is much "urban legend" commentary about Russian suitcase bombs and terrorist groups, the more recognized fear is a "dirty bomb" or a small bomb with radiological material as a component.[16] In the real world, the assassination of the ex-KGB agent Alexander Litvinenko in the streets of London in 2006 with polonium exposure raises the unsettling conclusion that either the incident was Russian state-sponsored, or a criminal gang was able to procure extremely dangerous and toxic radioactive material for the murder.[17] In fact,

> In the opening of Graham Allison's book, *Nuclear Terrorism,* Allison describes how the Central Intelligence Agency director, George Tenet, at the Presidential Daily Intelligence Briefing on October 11, 2001, informed President Bush that he had information that Al Qaeda had acquired a stolen Russian ten-kiloton nuclear bomb and that the source of the information believed the weapon was in New York City. According to Allison, in a moment of gallows humor, a staffer quipped that

---

[14] STEVE SHEPARD, A MURDER OF CROWS (Lyford Books) (1996).

[15] *Id.*

[16] Dan Vergani, *Experts close the lid on "suitcase nukes,"* USA TODAY, Mar. 12, 2007, at 9D, *available at* http://www.usatoday.com/tech/science/2007-03-12-suitcase-nuclear-bombs_N.htm (last visited Nov. 28, 2008).

[17] *See* Thomas de Waal, *Murder Most Foul: Following a deadly polonium trail from London back to Russia*, WASH. POST, July 27, 2008, at BW03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/07/24/AR2008072402621.html (last visited Nov. 28, 2008).

> the terrorists could have wrapped the bomb in one of the bales of marijuana that are routinely smuggled into cities like New York. The report proved to be false—this time.[18]

This Allison anecdote, for the purposes of this analysis, has the advantage of linking the contraband drug trade with terrorism in the violation of borders. As has been known for a long time, drug traffickers have been extraordinarily successful in penetrating our borders. In fact, the so-called "War on Drugs" has been successful in the sense that the street price for most drugs has remained low and accessible to the average street user.

Another threat to national security involving borders, although less popular and currently less recognized, is economic or industrial espionage.[19] In the words of Bernard Esambert, a president of the Pasteur Institute, "'Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor. . . the companies are training the armies and the unemployed are the casualties.'"[20]

When viewed from the perspective of National Counterintelligence Executive (NCIX), the governmental body charged with protecting economic security, trying to protect economic secrets in a world of shifting boundaries, world supply lines and spheres of influence is a monumental challenge:

> Boundaries of every kind are eroding—legally, behaviorally, electronically—in all aspects of our lives: Between the public

---

[18] Harvey Rishikof, *Long Ward of Political Order—Sovereignty and Choice: The Fourth Amendment and the Modern Trilemma*, 15 CORNELL J.L. & PUB. POL'Y 587, 587 (2006) (citing GRAHAM ALLISON, NUCLEAR TERRORISM: THE ULTIMATE PREVENTABLE CATASTROPHE (Times Books, Henry Holt & Co. 2004)). To see the effects of a ten-kiloton nuclear bomb, *see* www.nuclearterror.org. *Id.* at 587 n.2.

[19] *See* Harvey Rishikof, *Economic or Industrial Espionage—Who Is Eating America's Lunch? How Do We Stop It?*, *in* VAULTS, MIRRORS AND MASKS: REDISCOVERING U.S. COUNTERINTELLIGENCE (edited by Jennifer E. Simms & Burton Gerber, eds., forthcoming 2008).

[20] Wanja Eric Naef, *Economic and Industrial Espionage: A Threat to Corporate America?*, INFOCON MAGAZINE, Oct. 2003, *available at* http://www.iwar.org.uk/infocon/print/espionage-cid.htm (last visited Nov. 28, 2008).

> and private behavior of ordinary people; for example, the sense of dress and decorum appropriate to the home, the street, the office, or houses of worship. Between the public and private—that is, secret—behavior of governments. Between the financing, legal norms, and research activities of public as opposed to private institutions; [and] universities, for instance. Between state and non-state actors and the relative size of the resources they control. Cyber boundaries are also eroding—and not always in ways we like—but simply because we are sometimes helpless to enforce them.[21]

But those in government positions of authority are still responsible, and they have to try to craft a response to the new era of globalization, computerization, secrets and spying. The mission therefore is increasingly difficult and will not go away because the stakes are so high. In the elegant words of Joel Brenner, director of the NCIX, the "intellectual thieves" seem to have the upper hand at the moment.[22] As he recently explained at a public-private sector conference:

> The public and private sectors are both leaking badly. I'm not talking about just the pirating of DVDs and movies in Asia. I'm talking about significant technologies that are walking out of our laboratories on electronic disks, walking onto airplanes bound for foreign ports, and re-entering the country as finished products developed by foreign entrepreneurs. In effect, we're buying back our own technology. This is bad enough when we're talking about commercial innovation. But when we're talking about technology with substantial defense applications, we're talking about losses of intellectual capital that in wartime could cost many lives or our fellow citizens. These losses are occurring, and they are occurring in a targeted, systematic manner. Protecting innovative technology before it can be patented or classified is an urgent task, and it is difficult. If any of us knew how to do it, he'd be very rich,

---

[21] Dr. Joel F. Brenner, Welcoming Comments by Nat'l Counterintelligence Executive Dr. Joel F. Brenner, DNI—Private Sector Workshop on Emerging Techs. at Carnegie Endowment for Int'l Peace (Dec. 7, 2006), *available at* http://www.ncix.gov/publications/speeches/CarnegieSpeech20061207.pdf (last visited Nov. 28, 2008).

[22] *Id.*

because it's a question of handicapping basic research.[23]

The second set of propositions therefore is that the new threats are individualized, multivaried, potentially lethal on a mass scale, and potentially devastatingly costly on the economic ledger for research and development and competitive advantage. There is a clear and justified need for the state to patrol the borders so that both "blood" causing damages do not enter and economic "treasure" does not leave.

C. The Weberian Theory of The State: Consent—Authoritarian or Citizen Based—But State Power Remains

There are many ways to define a state for political and legal purposes. The *Weberian* definition for the purposes of the argument is the most helpful since it defines a state in legal and physical or geographical terms—"the *monopoly of the legitimate use of physical force* within a given territory."[24] The physical or territorial aspect of the definition is significant because it grants borders a special theoretical significance for a state's power. More significantly, the concept of citizenship is not part of the *Weberian* world of state definition since it centers authority on the legitimate use of force internally. The *Weberian* approach is essential to the Westphalian world of state powers, since internal domestic issues are excluded from the definition. Regardless of the process by which the monopolization of power is "legitimized," whether by democratic consent or authoritarian performance, a physical border must bound the state's writ. Physical borders therefore, have the potential to become special *legal areas* and the sovereign has particular powers over citizens and non-citizens alike, at the moment of entry. This approach is a fundamental challenge to U.S. jurisprudence, which has created a special and sophisticated jurisprudential framework for fundamental rights protection predicated on the idea of "citizenship," in contrast to an "authority" based concept of state

---

[23] *Id.*

[24] MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 154 (The Free Press 1964).

power.[25]

It is well recognized in political theory and comparative politics that the sovereign has special authority to protect the homeland and its people. One needs to underscore people, not citizens, since even today viable and significant states such as Saudi Arabia continue to have subjects, rather than voters. This core right to protect internally is enshrined in the democratic doctrines of "peace order and good government" in Great Britain[26] and *raison d'etat* in France.[27] Even our own U.S. Constitution has the "suspension clause" for the writ of habeas corpus, where in particular domestic emergencies such as rebellion or invasion the "public safety may require it."[28] Despite some views that the executive branch decides when to invoke the suspension, it is clear that this right to protect rests in Article I of the Constitution though the Supreme Court retains the role of deciding what constitutes a rebellion or invasion and when the public safety requires the state to ignore the core individualized writ of habeas.[29] Under the U.S. Constitution and the *Weberian* school of state power, it is an attack on the monopolization of power in the form of a rebellion or invasion which triggers the authoritative power of the state to trump the citizenship or individualized right of habeas. To be sure, under the U.S. Constitution, it is Congress (the institution most representative of the Madisonian factionalized interests) that makes the determination and not one individual as embodied in the office of the President; further, it is assumed that the suspension will be temporary or until public safety and

---

[25] *See* JOHN WILLIAM SALMOND, JURISPRUDENCE OR THE THEORY OF THE LAW 101 (Stevens & Haynes, 1907) (analyzing the essential role of citizenship in jurisprudence using the early legal common law).

[26] *See* Stephen Eggleston, *The Myth and Mystery of POGG (Peace order and good government)*, JOURNAL OF CANADIAN STUDIES, Jan. 1, 1996.

[27] Sir Herbert Butterfield, *Raison D'etat—The Relations Between Morality and Government*, Martin Wight Memorial Lecture at the University of Sussex 7 (Apr. 23, 1975) (transcript available at http://www.mwmt.co.uk/documents/butterfield.pdf).

[28] U.S. CONST. art. I, § 9, cl. 2 (The privilege of the writ of habeas corpus shall not be suspended, unless when in cases of rebellion or invasion the public safety may require it).

[29] *See* Boumediene v. Bush, Nos. 06-1195 & 06-1196, 2008 U.S. LEXIS 4887 (U.S. June 12, 2008).

order are restored.[30]

But, for the purpose of our propositions, this approach to the state establishes any state's core interest to control certain fundamental organs or functions that supersede its social contract of competing rights held by its citizens, subjects or members. From the perspective of the Bill of Rights, this *Weberian* state power to override all other rights is a dangerous and blunt authority that should be exercised sparingly and rarely. In fact, U.S. presidents have rarely invoked the Suspension Clause. But it is the proverbial loaded gun that is in the top drawer of any Congress that can be pulled out to allow the state to incarcerate when catastrophic disorder strikes. Moreover, the *Weberian* approach raises the legal potential for the government to claim that borders, due to the power of the state to exercise its authority with impunity, are special and unique locations where the authority of the state is paramount. Historically the borders were concrete, physical and could be demarcated with barriers of fences, flags, planes or ships.

To some critics the emerging world has become a struggle among three types of regimes of legitimacy—the autocratic economies (Russia and China), Islamic traditional states (Iran and Saudi Arabia) and the liberal democracies (U.S. and E.U.).[31] Needless to say, each group has its own internal rivalries but share certain norms and values. Each will continue to struggle to expand power and gather satellites for alliances and to maneuver for comparative advantage. But whither are domestic law and international law in this new world order? In 2006, Craig Allen, an international law professor, hosted a conference of international law experts to "vision" the future of the global legal order in 2020 at the Naval War College.[32] Allen boiled

---

[30] Note that when President Lincoln suspended the writ of habeas in the Civil War, he worked with Congress and went back to Congress after the fact for post facto approval of the legislature. *See* Lou Fisher, *Invoking inherent powers: a primer*, PRESIDENTIAL STUDIES QUARTERLY, Mar. 1, 2007, *available at* http://www.mywire.com/a/PresidentialStudiesQuarterly//3809872 (last visited Nov. 28, 2008).

[31] Robert Kagan, *The End of the End of History*, NEW REPUBLIC, Apr. 23, 2008, at 40.

[32] For a fuller description of the visions *see* Harvey Rishikof, *National Security Worldview*, THE REPORTER: THE JUDGE ADVOC. GENS. CORPS, Dec. 2006, at 152, 154-55.

down the possibilities of the current global legal order to six possible futures: no growth; slow growth; significant growth; the total disintegration of the order; the fracturing of the order into regional and bilateral arrangements; and, finally, no single future or an order of constant flux.[33] This flux extends to borders and domestic law.[34] In 2008, Russia violated Georgia's borders allegedly to protect the interests of minorities in South Ossetia,[35] while the United States in its war on terrorism crossed borders between Afghanistan and Pakistan under a doctrine of "hot pursuit."[36] How does one assert border control when international law and domestic law allow for "incursions" based on sovereign interpretations? What will citizens or subjects deem legitimate state action in the name of the common defense? Each regime of legitimacy—autocratic economies, Islamic fundamentalist and liberal democracy—views borders as unique areas of sovereign power that trump both domestic and international norms. The state's power is at its zenith, while the individual's zone of privacy and rights is at its nadir.

These propositions have created a social force of extreme state anxiety over border control since the evolving threat to its security (1) runs from economic espionage to weapons of mass destruction, (2) is potentially part of the world communication nodes and (3) is individualized, technologically connected, possibly tied to international criminal networks and centers on the transport of people and goods, the key to globalization. All of these forces and doctrines meet at the border under a state's domestic jurisprudence whereby traditional concepts of privacy stemming form citizenship are most challenged.

---

[33] *Id.*

[34] *Id.*

[35] Mikhail Gorbachev, *Russia Never Wanted a War,* N.Y. TIMES, Aug. 20, 2008, at A23, *available at* http://www.nytimes.com/2008/08/20/opinion/20gorbachev.html?_r=1&oref=slogin&pagewanted=print (last visited Nov. 28, 2008).

[36] Ron Synovitz, *Afghanistan: Legality Of 'Hot Pursuit' Into Pakistan Debated*, June 6, 2008, *available at* http://www.eurasianet.org/departments/insight/articles/pp062308_pr.shtml (last visited Nov. 28, 2008).

II. AMERICAN CONSTITUTIONAL LAW AND PUBLIC POLICY

A. Borders and the Fourth Amendment Strands: Whither Are U.S. Citizenship rights?

The concept of privacy has been an evolving idea in the jurisprudence of the United States. Central to the story has been the interpretation of the Fourth Amendment by the Supreme Court. In many ways our history and the government's attempt to assert order and control over illicit activity and defend against threats to the state by expanding its authority and seeking exceptions to the Fourth Amendment, has defined our contemporary view of privacy. Over the last 100 years, the fight against alcohol in Prohibition, the transportation of women for illicit purposes across state lines, the struggle against anarchism and communism, the anti-war movement, the war against drugs and the combating of terrorism have pitted law enforcement against the civil liberties community.[37] The Supreme Court has crafted rules of the road for law enforcement by setting limits and standards under the Bill of Rights. Critical to the dialogue are the exceptions that have been carved out to allow law enforcement to perform its duty. These exceptions to keep the state's power in check have been extensively litigated and debated. Over time, certain standards have been established to guide law enforcement when violating a citizen's privacy—probable cause, swearing out a warrant, reasonable suspicion and routine administrative searches. Border jurisprudence, however, has been an exception to this concept of privacy.

Professor Thomas K. Clancy has noted that the expansive state border authority has long historical roots; the first customs statute predates the Bill of Rights and allowed for warrantless inspections of vessels.[38] Modern day jurisprudence has similarly

---

[37] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. R. 349 (1973-74).

[38] *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 404, n.22 (2008). *See also* 19 U.S.C. § 482 (2008) (originally enacted as Act of July 18, 1866, ch. 201, § 3, 14 Stat. 178); Immigration and Nationality Act § 287, 8

rejected traditional tests of the totality of the circumstances or heightened levels of suspicion, or minimal indications, or clear indications, or plain suggestions, or articulate suspicion.[39] As Professor Clancy has underscored, for "intrusive" searches and seizures at the border, reasonable suspicion is required.[40] But intrusive has been interpreted to mean unreasonable invasions of the body (body cavity searches, strip searches and x-ray treatment, unless there are facts to give rise to heightened suspicion)[41] or significant damage to property. Border officials, based on training and experience, can conduct a form of targeting that is initially focused on demeanor but then is followed by more extensive investigations, routine "pat downs," searches and inquiries. Federal officers with customs or immigration enforcement authority possess unique power as agents of the state. As has been long noted by courts and traditional law enforcement:

> Congress has given the authority to conduct border searches *only* to this limited group of officials [customs or immigration], and has charged them with the exclusive responsibility for inspecting goods and persons crossing the borders and for interdicting illegal entries. Searches conducted by other law enforcement agents are not considered border searches, . . . and must therefore meet the traditional demands of the fourth amendment.[42]

U.S.C. § 1357 (2008).

[39] *See* United States v. Ramsey, 431 U.S. 606, 619 (1977) (stating that border search exception is older than the Fourth Amendment). *See also* United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985) ("Having presented herself at the border for admission, and having subjected herself to the criminal enforcement powers of the federal government, 19 U.S.C. § 482, respondent was entitled to be free from unreasonable search and seizure."). In *Montoya*, Ms. Hernandez was detained for sixteen hours and had to excrete into a wastebasket since she was suspected of alimentary canal smuggling. *Id.* at 531.

[40] CLANCY, *supra* note 38, at 407.

[41] United States v. Flores, 477 F.2d 608, 609 (1st Cir. 1973) (holding discovery of numerous undeclared emerald stones sufficient for strip search); *see also* YULE KIM, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT (CRS Report, Order Code RL 31826) (updated Jan. 15, 2008).

[42] United States v. Sandoval Vargas, 854 F.2d 1132, 1136 (9th Cir. 1988) (citing United States v. Soto-Soto, 598 F.2d 545, 550 (9th Cir. 1979)).

The customs official's special power to search "vehicles" and "packages" at borders without individualized or reasonable suspicion has been reinforced in the Ninth Circuit by broadly applying 19 U.S.C. § 1581 which allows (1) the search, examination and inspection of vessels and vehicles and (2) examination of manifests, documents, papers, person, trunk, package or cargo on board.[43]

The doctrine has also pushed out the location of borders or extended them. Already in 2004 in one FBI Law Enforcement bulletin the notion of an extend border doctrine was described as follows:

> The extended border doctrine provides that non-routine border searches that occur near the border are deemed constitutionally permissible if reasonable under the Fourth Amendment," something which is determined by a three-part test, "whether 1) there is a reasonable certainty [or a high degree of probability] that a border crossing has occurred; 2) there is a reasonable certainty that no change in the condition of the luggage [i.e., the item or person to be examined] has occurred since the border crossing; and 3) there is a reasonable suspicion that criminal activity has occurred." (50) This three-part test becomes necessary in an extended border search context because it "entails greater intrusion on an entrant's legitimate expectation of privacy than does a search conducted at the border or its functional equivalent[.]" (51) What, however, is reasonable certainty? This is a proof threshold that lies between probable cause and beyond a reasonable doubt. (52) Regarding the second prong of the test, key to concluding whether or not there has been any change in the luggage, conveyance, or any other item, because it crossed the border are factors including "the time and distance from the original entry and the manner and extent of surveillance." (53) The signal characteristic that differentiates the extended border search from one conducted at the border's functional equivalent is that the first "takes place after the first point in time when the entity might have been stopped within the country." (54) Significantly, a proper extended border like a functional

---

[43] *See* United States v. Taghizadeh, 41 F.3d 1263 (9th Cir. 1994); United States v. Flores-Montano, 424 F.3d 1044 (9th Cir. 2005).

equivalent search may take place without either a warrant or probable cause.[44]

---

[44] *See* M. Wesley Clark, U.S. Land Border Search Authority, Aug. 2004, *available at* http://findarticles.com/p/articles/mi_m2194/is_/ai_n6232025 (last visited Nov. 4, 2008) (internal quotes omitted). Clark's footnotes contained within the above quotation also provide insight regarding this doctrine and are therefore quoted below:

(50) Yang, 286 F.3d at 945 (emphases added; citations omitted). Of course, one can substitute whatever "container" is at issue for the term luggage. See also United States v. Espinoza-Seanez, 862 F.2d 526, 531 (5th Cir. 1988). The third prong of the extended border test, reasonable suspicion of criminal activity, can arise from a number of factors, to include: "1) characteristics of the area in which the vehicle is encountered; 2) proximity to the border; 3) usual patterns of traffic on the road; 4) previous experience with alien traffic; 5) information about recent illegal crossings in the area; 6) behavior of the driver; 7) appearance of the vehicle; and 8) number, appearance, or behavior of passengers." Espinoza-Seanez, supra at 531; see also Cardenas, 9 F.3d at 1148; cf. Cardona, 769 F.2d at 629 (totality of circumstances test adopted for extended border searches) (citations omitted).

(51) Yang, 286 F.3d at 946 (defendant accosted after he had cleared international arrival terminal, his luggage having been x-rayed with negative results, and had traveled to a separate terminal via airport tram; second look, deemed proper as extended border search, uncovered opium-soaked clothing).

(52) Id. at 947 (citations omitted).

(53) Id. at 948 (citations omitted); see also United States v. Fogelman, 586 F.2d 337 (5th Cir. 1978) (extended border search permitted 254 miles and 20 hours from observed border crossing); United States v. Martinez, 481 F.2d 214 (5th Cir. 1973) (extended border search allowed 150 miles and 142 hours after border was crossed). "[C]ontinuous surveillance is not a requirement of an extended border search[.]" Cardenas, 9 F.3d at 1150, and thus a break in that surveillance is not fatal to the conduct of an extended border search. "The government is not required to negate every hypothetical possibility as to how the contraband may have been obtained subsequent to the border crossing. [T]he mere assertion by the defendant that there was the opportunity to obtain contraband after the border crossing is insufficient to controvert the facts established by the government." Id. at 1152, quoting from Ramos, 645 F.2d at 321 (30-minute break in surveillance does not defeat application of extended border search doctrine). Note that some courts may be confusing functional equivalent and extended border searches. "The 'functional equivalent' subcategory includes searches made at points inland of national borders under circumstances other than continuous surveillance that guarantee preservation of border-crossing conditions at the point of search. The underlying principle that permits them to be treated as border searches is thus the same as that for extended border searches. Courts may in fact be using the terms interchangeably." Bilir, 592 F.2d at 742 n.11.

(54) Cardenas, 9 F.3d at 1148 (original emphasis). There is one characteristic that routine border, border functional equivalent, and extended border searches all have in common: the person, conveyance, or item to be searched "brings the border with it to the point of the search." Id. at 1149 (internal quotation marks and citations omitted).

This physical extension of the border relies heavily on the assumption that surveillance has been able to satisfy the three-pronged test. This notion of extending the physical border has a potential analytical equivalent in the computer world. Moreover as the court established in *United States v. Flores-Montano*, at the border, as part of a routine search, customs officials can dismantle, remove and reassemble a vehicle's fuel tank.[45] As part of the Court's analysis, *Flores-Montano* noted that the search allowed for reassembling and not destruction.[46] The cache of information contained in computers and the possibilities of potential threat enhanced by the justification of border explorations of data presents a powerful potential clash of doctrines.

B. The Clash of the Doctrines?:[47] Extending the Digital Legal Border—All Is Flux

One of the more unfortunate analogies of the post 9/11 era is the alleged hunt "to connect the dots" to thwart any future terrorist attack on continental United States (CONUS).[48] At the outset one must begin with the premise that given the openness of modern society it is virtually impossible to stop all terrorist attacks. The recent histories of attacks in Spain, Great Britain, Israel and France make this premise painfully clear.

Further, any analysis of the cargo shipping industry and its current state of protection, as documented by Stephen Flynn from the Council on Foreign Relations, should underscore his message that resiliency of our infrastructure, not prevention alone, must be the wise policy in the area of combating

---

[45] 541 U.S. 149, 155 (2004).

[46] *Id.* at 152.

[47] Section drawn from Harvey Rishikof, *The "War on Terror" and Prevention: Improving the Domestic Paradigm for the Digital Age*, NAT'L STRATEGY F. REV., Winter 2007, *available at* http://www.nationalstrategy.com/Programs/NationalStrategyForumReview/PastNSFRIssues/Winter2007NSFRV171/tabid/112/Default.aspx (last visited Nov. 28, 2008).

[48] CNN.com, Testimony of Secretary Condoleezza Rice before the 9/11 Commission, Apr. 8, 2004, *available at* http://www.cnn.com/2004/ALLPOLITICS/04/08/rice.transcript/ (last visited Nov. 28, 2008).

terrorism.[49] With these caveats in mind, the domestic paradigm for investigation of terrorism in the digital age has many facets to which the border exception to the Fourth Amendment provides a heuristic legal and policy analogy.

The current situation of digital investigation is one of a state of flux. Fourth Amendment jurisprudence, data mining, executive authority, war paradigms, due process, border exceptions and judicial review have become a tangled mess for the protection of privacy. In the words of one commentator, modern Internet searches lie at the intersection of telecommunications, spy technology and the statutory regimes that govern surveillance.[50]

It is often said that the U.S. Constitution is a document of enumerated powers, separation of powers, emergency powers and protected rights.[51] The attack on 9/11 has tested competing constitutional theories over where authority lies among these competing powers to respond to the threat of terrorism. Over the last six years this debate has spawned a flurry of legislation, reforms and new institutions—e.g., the PATRIOT Act, Intelligence Reform Acts, a new Department of Homeland Security, a new Director of National Intelligence, a new National Security Branch for the Federal Bureau of Investigation, a secret surveillance program, a new Homeland Security Council and most recent, the Protect America Act. Currently, debate swirls around the new proposed legislation titled the Restore Electronic Surveillance That is Overseen, Reviewed and Effective Act (RESTORE).[52]

Given all these changes, has the United States improved detection, prevention and response? Is more institutional

---

[49] STEPHEN E. FLYNN, EDGE OF DISASTER (2007). Flynn has written extensively on infrastructure security and the importance of resiliency since it is impossible to secure borders given the volume of traffic and the nature of our modern threats.

[50] Barton Gellman, *Conflict Over Spying Led White House to Brink*, WASHINGTON POST, Sept. 14, 2008, at A1, A14.

[51] Robert F. Turner, *The Supreme Court, Separation of Powers, and the Protection of Individual Rights during Periods of War or National Security Emergency*, 28 J. SUP. CT. HIST. 323 (2003).

[52] RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM (Rowman & Littlefield Publishers Inc., 2006).

change needed and how should Fourth Amendment jurisprudence respond? Moreover, has the United States appropriately resolved the tension between civil liberties and investigation? The short answer to these questions is that more change is required and civil liberties may not have been adequately protected.[53]

As outlined in the first part of the paper, over the next few decades there will be certain technological constants. Increasingly, the private sector—telecommunications companies, banks, insurance companies and credit card companies, etc., will be amassing ever larger and more detailed information data banks on U.S. citizens. These ever growing data banks will be subject to even more powerful "search engines" that will able to be "banged" for more connections, relations and ties. It will be the private sector, and not the government, that will be the repository of this critical information.

This information will be carried across borders and sent across borders as digital data by individuals and corporations.[54] The logic of the "data bank banging" argument is that finding terrorists in a sea of information is analogous to the Cold War problem of trying to find Soviet submarines hidden in plain view in the ocean. The solution was to monitor the ocean under normal circumstances and then to register "disturbances." In fighting terrorism the analogy is that a group involved in a conspiracy would emit "patterns of behavior" or "signatures" that would similarly "disturb" the regular flow of commercial behavior and traffic flow. These "patterns" could be identified, and algorithms could be fashioned to pick them out of the sea of "normal" commercial transactions. To be successful though, a "sea" of information is required. This approach was behind the Total Information Awareness Program (TIA) established at the Department of Defense's Defense Research Projects Agency (DARPA) that caused a political firestorm when it was

---

[53] *See, e.g.*, Symposium, *Left Out in the Cold? The Chilling of Speech, Association, and the Press in Post-9/11 America*, 57 AM. U. L. REV. 1197 (2008).

[54] *See supra* text accompanying note 23.

revealed.[55] The goal of the TIA program was "to create a counter-terrorism information system that: (i) increase[d] the information coverage . . . (ii) provide[d] focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; [and] (iii) [could] automatically cue analysts based on partial pattern matches and analytical reasoning, and information sharing . . . ." [56] As outlined by the Congressional Service Report:

> DARPA's five year research project to develop and integrate information technologies into a prototype system for use by the intelligence, counterintelligence and law enforcement communities intends to exploit R&D efforts that had been underway for several years in DARPA and elsewhere, as well as private sector data mining technology. DARPA envision[ed] a database "of an unprecedented scale, [that] would most likely be distributed, must be capable of being continuously updated, and must support both autonomous and semi-automated analysis." . . . Extensive existing databases from both private and public sector information holdings [would have been] used to obtain transactional and biometric data. Transactional data for the TIA database could include financial (*e.g.*, banks, credit cards, and money transmitters, casinos and brokerage firms), educational, travel (*e.g.*, airlines, rail, rental car), medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, government, and communications (*e.g.*, cell, landline, Internet) data. Biometric data for the database could include face, finger prints, gait, and iris data. The TIA system could seek access to databases to discover connections between "passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases—and events—such as arrest or suspicious

---

[55] *See* ACLU, Stunning New Report On Domestic NSA Dragnet Spying Confirms ACLU Surveillance Warnings, *available at* http://www.aclu.org/privacy/gen/34441prs20080312.html (last visited Oct. 10, 2008) (ACLU's response to the TIA).

[56] *See* Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, CONG. RES. SERV., Mar. 21, 2003, at 2, *available at* http://www.fas.org/irp/crs/RL31730.pdf (last visited Oct. 22, 2008) (citations omitted).

activities and so forth."[57]

In the end Congress requested that the program be stopped—but the logic that underlies the approach lives, and border crossing has become the next focal point of the debate for information gathering.[58]

C. Electronic Surveillance, Searches and Foreigners

If prevention of terrorism, however, is the goal of the state, then timely information to thwart actions is the key to success. The recent debate over the RESTORE legislation is a perfect example of the interrelated issues of data mining, prevention and digital borders.[59] The new National Security Letters, for example, granted to the FBI under the PATRIOT legislation, allow local agents to request data, without any court order, from the private sector.[60] In short the border for information acquisition was moved, without judicial supervision, closer to executive discretion.

Domestically the debate asked various questions related to the proper legal procedure for acquiring access to these data banks: Should the executive branch [on its own authority to protect the republic] be able to request the records in order to search them without judicial oversight? Should the private

---

[57] *Id.* The federal laws triggered by the approach included the following: The Privacy Act of 1974, The Family Educational Rights and Privacy Act of 1974, The Cable Communications Policy Act of 1984, The Video Privacy Protection Act of 1988, Telecommunications Act of 1996, The Health Insurance Portability and Accountability Act of 1996, Driver's Privacy Protection Act of 1994, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, The Foreign Intelligence Surveillance Act of 1978, The Electronic Communications Privacy Act of 1986, The USA PATRIOT Act of 2001, The Homeland Security Act of 2002, The Fair Credit Reporting Act of 1970, The Right to Financial Privacy Act of 1978, The Gramm-Leach-Bliley Act of 1999, and The Children's Online Privacy Protection Act of 1998. *Id.* at 6-16.

[58] *See* JAMES BAMFORD, THE SHADOW FACTORY, THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA, (Doubleday, 2008) (discussing the latest revelations concerning the National Security Agency).

[59] *See* ThinkProgress, *available at* http://thinkprogress.org/restore-act-summary/ (last visited Oct. 21, 2008) (providing summary of the RESTORE Act of 2007).

[60] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 18 U.S.C. § 2709 (2008), *invalidated by* Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

companies that cooperate be able to be sued, or should they be granted immunity from lawsuits? What level of suspicion should be required before access is granted to these data bases—individual, as traditionally required by the Fourth Amendment, or a more general class identification (e.g., all the records from all the hotels in Las Vegas where a threat to the city is suspected)? The RESTORE debate wrestled with these questions.[61] In effect, the debate from the government's perspective was an attempt to philosophically extend digital "border" protection to the interior of the state.

Politically, this constitutional question of the governmental right to search, and under what standard of review, will continue to bedevil any administration that plans to combat terrorism. Where will the constitutional authority lie and what should be the role of the courts in the process? In the physical border context the discretion falls on the border agents. Proponents of a strong executive argue that when the state is at war, such as the war on terrorism, the commander-in-chief has constitutional authorization to initiate terrorist surveillance programs based on his inherent authority.[62] This inherent authority trumps all restraints, even if Congress has legislated in the area and mandated judicial review of the process.[63] This approach grants and extends custom and immigration warrantless search authority inwards and erodes the U.S./non-U.S. distinction that has been such a vital component of our constitutional framework.

Opponents to this position reason that this is a congressional prerogative and once Congress has established the rules to govern the situation, the president is bound to follow them, or risk censure, or even impeachment. For this view of constitutional power, unchecked executive power in the defense

---

[61] *See, e.g.*, The Huffington Post: Blog of U.S. Rep. Rush Holt, *available at* http://www.huffingtonpost.com/rep-rush-holt/whats-really-in-the-rest_b_74309.html (Nov. 27, 2007, 12:33 EST).

[62] *See, e.g.*, Dawn E. Johnson, *What's a President to Do? Interpreting the Constitution in the Wake of Bush Administration Abuses*, 88 B.U. L. REV. 395, 395-96 (2008) (criticizing the position).

[63] *Id.*

of liberty results in problems such as the Palmer raids of the 1920s, the miscarriage of justice under the McCarthy era in the 1950s, and the violations of civil liberties uncovered by the Church Committee in the 1970s.[64] In fact, to many it was these very executive violations that spurred Congress to pass the Foreign Intelligence Surveillance Act (FISA) in 1978.[65]

FISA, however, was drafted in an era before the technological revolution of the Internet and when a separation of domestic and foreign arenas was taken for granted. At the heart of the FISA legislation was the distinction between a U.S. citizen and a non-U.S. citizen. In many ways technology, the U.S./non-U.S. citizen distinction and the separation of domestic and foreign spheres has been undermined by the evolution of communication and the nature of the evolving threat. FISA envisioned a world of states v. states, not a world of stateless actors working in cooperation to attack CONUS, with some of the enemies potentially being U.S. citizens. This type of threat that has been successful in Spain and Great Britain is a challenge to the old order and legal structures. Border jurisprudence, as part of our founding, never distinguished between U.S. and non-U.S. citizens in the Fourth Amendment sense. At the border U.S. citizens have a reduced sense of Fourth Amendment protection. The debate of what protection a computer has at the border is one that raises legal issues over how to understand what digital datum is. Again, Professor Thomas K. Clancy has elegantly argued that electronic data on a computer does not require a "special approach" and should be governed by traditional Fourth Amendment rules regulating containers and document searches.[66]

FISA's solution was, when dealing with non-U.S. citizens, to involve the federal judiciary to curtail executive power in the area of foreign persons or agents of foreign entities. In a system parallel to the criminal process, where search warrants

---

[64] *See* DAVID COLE, ENEMY ALIENS, (W.W. Norton & Co. photo reprint 2005) (2003).

[65] *See* Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C. & 18 U.S.C. §§ 2518-2519).

[66] Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005).

requiring probable cause of a crime obtained from a federal judge are needed, FISA requires probable cause of a "foreign agent" before surveillance can be established.[67] The lack of U.S. status became the critical threshold before monitoring could take place. What has changed for proponents of executive power to argue that the judiciary should not be involved in this procedure? In short, the government claimed that it stood in the shoes of a customs or immigration official and that at the technological border—no Fourth Amendment was a bar to state action.

The position to exclude the judiciary in the process of monitoring surveillance rests on arguments of constitutional authority and necessity. First, proponents argue that the United States is at war and this authority to protect is a presidential right that cannot be curtailed.[68] If the President approves the authorization it is constitutionally appropriate under his emergency war powers. Second, proponents believe that judges lack the institutional competence to second-guess the executive on its judgments when the United States is at war and when protection of the homeland is paramount.[69] Third, in this era of technological information, speed, surveillance and data mining are the keys to prevention, and proponents argue this too is beyond the judiciary's competency.[70] The world of exploiting information has changed and the judicial review is not useful, since a deliberative procedure is the antithesis of prevention based on speed of action and establishing connections.

The response to these arguments is a flat rejection of the premises for each of the positions. Philosophically, supporters of the judiciary are wedded to the Madisonian principle of checks and balances. No branch, when civil liberties are involved,

---

[67] *See* 50 U.S.C. § 1802(a)(1)(A) (1978).

[68] See, John Yoo, *Exercising Wartime Powers The Need for a Strong Executive*, HARV. INT'L REV., *available at* http://www.harvardir.org/articles/1369/1/ (last visited Nov. 28, 2008).

[69] *See* The Federalist Society Online Debate Series, FISA, Dec. 11, 2007, *available at* http://www.fed-soc.org/debates/dbtid.13/default.asp (last visited Nov. 21, 2008).

[70] *Id.*

should be granted sole authority. To this school, terrorism is more of a criminal matter rather than one of war. Europe has taken this approach by passing expanded criminal statutes to combat terrorism.[71] For the Madisonian proponents, the judiciary should be second-guessing the executive. This school points to the violations of the FBI in using National Security Letters, as documented by the Inspector General of the Department of Justice, to underscore why the judiciary must be part of the process.[72] Finally, on the issue of speed, the proponents for the role of judges reason there are ways to expedite the processes. After the fact, once decorum has been reestablished, a backward-looking review under judicial scrutiny can be undertaken to right any wrongs.

After months of negotiations and wrangling on these issues, Congress secured passage of the Foreign Intelligence Surveillance Act of 2008 (FISA/2008).[73] Critics of the Act have focused on several issues: the retroactive civil and criminal immunity granted to telecommunications corporations for compliance with executive requests that arrived without court orders; the more restricted certification process for the reviewing FISA court; the broader "dragnet" broadband authorization for information; and the expanded reporting time granted the government.[74] Defenders of the legislation emphasize the clear statement that the new FISA/2008 is the "exclusive means" for intercepting electronic communications; increased congressional oversight; the enhanced protections for U.S. citizens living overseas; and the new enhanced role of the inspector general to

---

[71] *See* Prepared Remarks of Attorney General Alberto R. Gonzales at the Vienna E.U. Interior Ministers Conference, May 5, 2006, *available at* http://www.usdoj.gov/archive/ag/speeches/2006/ag_speech_060505.html (last visited Nov. 21, 2008).

[72] *See A Review of the FBI's Use of National Security Letters*, DEP'T OF JUSTICE SPECIAL REP., Mar. 2008, *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf (last visited Nov. 28, 2008).

[73] *See* The FISA Amendments Act of 2008, 50 U.S.C. § 1802 (1978), *amended by* H.R. 6304 (2008).

[74] *See* ACLU website *at* http://www.aclu.org/safefree/general/17321res20030408.html (last visited Nov. 28, 2008).

review the government's actions.[75]

Regardless of where one breaks on the issues, there appears to be a consensus that FISA needs to be modernized to account for the new technologies and developments in the communications arena. The "old" FISA of 1978 was written for a world of phones, routers and telegraphs with limited traffic capacities and specific locations whereby one could clearly delineate foreign and domestic. The brave new world of web-based communications has revolutionized technical mechanisms, delivery modes, locations, storage banks and volume. The lapsing stop-gap Protect America Act, the limited fix to FISA, recognized that something new was needed.[76] A new approach was required for an increasingly borderless world of communications, mobile citizenry and data storage facilities.

Knowable individualized surveillance versus general broadband collection is an essential part of the debate—who will authorize the broadband collection, by what standards, and who will review the authorization and monitor the collection? This is often referred to as the "minimization" issue—in short, how and who will keep the executive accountable. As David Kris, a former Associate Deputy Attorney General who has written extensively on national security issues and surveillance, has pointed out FISA/2008 has three essential substantive requirements: first, a target that is a foreign power or an agent of a foreign power; second, a facility being used by that target; and third, minimization.[77] To satisfy these requirements without sacrificing speed and agility, it is necessary to identify the broadest possible target and facility, which will yield the broadest possible authorization order and require the fewest

---

[75] CRS Report, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, June 12, 2008 (RL 34533), *available at* http://www.fas.org/sgp/crs/intel/RL34533.pdf (last visited Nov. 28, 2008).

[76] *See Fact Sheet: The Protect America Act of 2007*, OFF. PRESS SEC'Y, Aug. 6, 2007, *available at* http://www.whitehouse.gov/news/releases/2007/08/print/20070806-5.html (last visited Nov. 28, 2008).

[77] *See* Posting of David Kris to Balkinization, *available at* http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-i.html (June 21, 2008, 8:50 EST).

possible court orders for the most surveillance.[78]

These facilities or international gateway switches have enormous amounts of data and traffic. But the status of the origin of the communication, the nationality of the communicator and the storage location of the data challenged the old FISA categories of target and facility. What are domestic-to-domestic versus international-to-domestic versus international-to-international communications? Imagine an American traveler who lends his iPhone to a French friend to make a call from Germany to his friend in Yemen. This call would now require a FISA warrant if the American was a target.

The Bush administration, confronted with the problem of identifying the nationality of the communicator, the location of the communicator, the place of the "facility" and volume of the data, chose to ignore the old FISA.[79] The administration asserted executive presidential prerogative to use the foreign power/foreign origin of the communication to assert that it did not need a FISA warrant to secure the data from the owners of the international gateway switches and stored data banks.[80] The potential threat, the administration reasoned, warranted swift action.[81]

The next step was to use "filters" or "data searches" to find the communication network needle in the haystack. Under the minimization doctrine and the new act, the government is to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[82] But if the data is "foreign intelligence information" or is "evidence of a crime which has been, is being, or is about to be committed," it can be retained and acted upon.[83] This has raised concerns in the civil

---

[78] *Id.*

[79] *See* Julian Borger & Suzanne Goldenberg, *Defiant Bush Defends Wiretapping Powers*, THE GUARDIAN, Dec. 20, 2005, *available at* http://www.guardian.co.uk/world/2005/dec/20/usa.topstories3 (last visited Nov. 28, 2008).

[80] *Id.*

[81] *Id.*

[82] *See* 50 U.S.C. § 1801(h) (1978).

[83] *See* 50 U.S.C. § 1802 (1978), *amended by* H.R. 6304 (2008).

liberty community about how much information these sweeps will gather.

The new FISA is an attempt to bring back accountability and review of governmental action in this complex technical area of electronic surveillance in the digital age. But as this brief review has highlighted, it is the technology that has made obsolete so many of the categories of the old FISA. The concept of U.S. citizen is harder to determine in this interconnected world of mobile communications and storage capacities. The modern world is creating enormous data banks of information controlled by the private sector. The government is only a warrant or a subpoena away from this vast ocean of information on its citizens and visitors. All governments are wrestling with the problem of how, under the rule of law, information should be obtained, searched, protected and not be the subject of governmental abuse. The new FISA statute is the most recent attempt to resolve these problems, but many questions remain to be answered as the intelligence community begins to "operationalize" the new rules.

The data is there in the private sector. Technology allows for more extensive and detailed searches. The goal is to prevent the threats; the government is held accountable for failures. As one can see, the FISA debate is more than a debate about technology, modern surveillance and executive accountability. At the heart is the erosion of citizenship as a shield to government intrusion and what privacy means in the new age. Congress has entered the fray again with more review; the IGs are part of the process; and the FISA court's authority has been reinstated. The hope is that more judicial review will provide enough accountability; but, a new president will have to see if the framework is adequate.

D. Are We At War?: If So, What Kind of War?

Since the passing of the Authorization for the Use of Military Force (AUMF) by joint resolution of the Congress in 2001, the invasion of Afghanistan, Iraq and by incursions into Pakistan, the Administration has contended the republic is at

war.[84] Most significantly for the theory of the clash of doctrines, the AUMF for the first time in U.S. history, authorized "all necessary and appropriate force" against "those nations, organizations, or persons" the President determined were responsible for the acts and similar force to prevent the occurrence of future acts. The power of the state could be focused on specific individuals; this was a fundamental change in how, and from whom, threats were conceived. In essence, the AUMF has ushered in a new paradigm of conflict and state power.

For it is an old saw that military or security "necessity" justifications, when civil liberties are encroached, should be viewed with a "healthy skepticism."[85] As has been pointed out by Judge James E. Baker in exploring the meaning of national security, there is "no single definition of national security" recognized in law or policy and "[s]ecurity is concrete [while a] [r]ule of law is an abstraction, a term that is easy to employ in rhetoric, but hard to measure in result."[86] As underscored by

---

[84] Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001). AUMF reads in relevant part as follows:

> To authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States. Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it . . .
>
> SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.
>
> (a) IN GENERAL- That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

[85] *See* Brown v. Glines, 444 U.S. 348, 369 (1980) (Brennan, J., dissenting).

[86] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 18, 22 (Cambridge University Press 2007).

Baker, Justice Jackson once famously opined, "a judge . . . may be surprised at the poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves."[87] Faced with the dilemma of "concrete security" versus "abstraction in law," policy makers are prone to choose the concrete at the expense of abstraction. But again, Baker's words are prescient:

> . . . a national security policy that does not include the rule of law as a core element will diminish not only our liberty but also our security. That is because good process, founded in law, including good legal process, as well as good faith adherence to the law, produces better security results.[88]

From the founding of the republic, Alexander Hamilton in Federalist Paper No. 8 judiciously warned that it is the nature of war to increase the executive at the expense of the legislative authority.[89] How to avoid this executive expansion of power under the cloak of security necessities? One answer is a full vetting process by the executive whereby all affected parties have an opportunity to voice views. Baker previewed the recent legislation on electronic surveillance in his review of constitutional law as applied. In a creative chapter, Baker (in lawyer-like fashion) lays out the legal arguments for and against presidential authority to authorize warrantless surveillance under the Foreign Intelligence Surveillance Act (FISA). He based his arguments on an analysis of the legal categories of a constitutional framework/court precedents/wartime powers and responsibilities/historic practices/statutory analysis under FISA, the Authorization to Use Military Force (AUMF), and facts.[90] This analysis is followed by an equally powerful "legal policy advice" section presenting the prudential factors in determining the President's position to exercise "inherent executive power" based on secrecy, efficiency, presidential authority and

---

[87] *Id.* at 47.

[88] *Id.* at 22.

[89] THE FEDERALIST NO. 8 (Alexander Hamilton).

[90] BAKER, *supra* note 86, at 71.

legislative tactics.[91] Again he explores in the alternative, the following of a parallel track with the legislature or judiciary based on rule of law and public diplomacy/sustained public support/maximization of presidential authority/encouraging risk-taking with legislative backing/ and most prophetically private sector protection and support.[92] The point is a deliberative process with checks and balances. If the new electronic frontier borders require surveillance, then Congress, as it recently has done, must involve the judiciary as a check on potential executive abuse. In the alternative, the executive, when perceiving catastrophic threats will opt for a physical border approach and push for more Fourth Amendment exceptions.

But the issue remains when at the border with a computer: What are the government's interests, and what is a reasonable expectation of privacy? Moreover, if the data is encrypted, by what manner should the border guards be able to request the password? Under the container theory, encryption is analogous to a lock, and failure to provide the key allows border detention and refusal to be admitted. The levels of issues range from national security justifications, to stopping pornographers, to new creative ways to launder money using Second Life programs, to economic espionage.[93] Computers at the border potentially contain material for all of these threats and crimes. The issue of computers at the border raises questions of sovereignty, technology, citizenship, national security, and privacy rights. In short, it presents a clash of legal and political doctrines over sovereignty and the limits of state power over the individual.

E. Smart Borders: Immigration, Privacy and Rights

It is instructive in understanding this clash of doctrines to

---

[91] *Id.* at 94.

[92] *Id.* at 95.

[93] *See* John S. Grant IV, *The New Frontier in the Fight Against Online Economic Scams and Internet Threats to Children: Virtual Worlds and Second Life*, CYBERCRIME NEWSLETTER, July-Aug. 2008, at 3.

review the latest advice from the National Counterintelligence Executive Office (NCIX) on what you should know when traveling overseas with mobile phones, laptops, PDAs and other electronic devices. In other words, how our friends and foes are treating borders and searches:

> • In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel businesses centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
>
> • All information you send electronically—by fax machine, personal digital assistant (PDA), computer, or telephone—can be intercepted. Wireless devices are especially vulnerable.
>
> • Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this remove the battery.
>
> • Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
>
> • Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."
>
> • Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
>
> • Corporate and government officials are most at risk, but don't assume you are too insignificant to be targeted.
>
> • Foreign security services and criminals are adept at "phishing"—that is, pretending to be someone you trust in

order to obtain personal or sensitive information.

> • If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device's hard drive has been copied.[94]

This advice is both disturbing and an insight into how the intelligence community understands borders and technology in the twenty-first century. This sense of vulnerability has also encouraged a refocus on travel documents since "[f]or terrorists, travel documents are like weapons."[95] The Department of Homeland Security, in an attempt to secure borders and identification, supported the REAL ID Act of 2005[96] and the Western Hemisphere Travel Initiative (WHTI).[97] As a result, in 2007 more than 30,000 individuals were detained at ports of entry trying to cross the border with false documents.[98] Under the REAL ID Act, each card must include, at a minimum, the person's full legal name, signature, date of birth, gender and

---

[94] Tips from the National Counterintelligence Executive, *Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices*, NCIX, Aug. 5, 2008, *available at* http://www.ncix.gov/whatsnew/index.html (last visited Nov. 28, 2008).

[95] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 108TH CONG., 9/11 COMMISSION REPORT 384 (Comm. Print 2004).

[96] Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami
Relief, Pub. L. No. 109-13, 119 Stat. 231 (2005); *see also* The Legislation Behind a National ID, CNet News, *available at*
http://news.cnet.com/The-legislation-behind-a-national-ID/2100-1028_3-6228910.html?tag=txt (last visited
Oct. 27, 2008). For example, in 1995 Timothy McVeigh, the Oklahoma bomber of the Murrah Federal Building, created a fake South Dakota driver's license using a manual typewriter and a kitchen iron. He then used this fake license to rent the Ryder truck he filled with explosive material. Baker, *infra* note 97.

[97] Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec., Statement for the Record Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, United States Senate, (April 29, 2008), *available at* http://hsgac.senate.gov/public/_files/BakerTestimony042908.pdf (last visited Nov. 28, 2008).

[98] *Id.* at 4.

driver's license or identification card number.[99] It also includes a photograph of the person's face and the address of principal residence, as well as physical security features designed to prevent tampering, counterfeiting or duplication of the document for fraudulent purposes.[100] Although the DHS denies that the REAL ID Act creates a national identification card, critics contend that the law places no limits on potential required uses for Real IDs. The fear is that in the future:

> Real IDs could be required to vote, collect a Social Security check, access Medicaid, open a bank account, go to an Orioles game, or buy a gun. The private sector could begin mandating a Real ID to perform countless commercial and financial activities, such as renting a DVD or buying car insurance. Real ID cards would become a necessity, making them de facto national IDs.[101]

Would the creation of a national ID card be the end of privacy? Many democratic European countries have had national IDs for decades and are introducing new "biometric IDs," but how would the national IDs be monitored by the state?[102]

Under the WHTI Air Rule all arriving air travelers, regardless of age, are required to present a passport or other acceptable secure document for entry into the United States. Since the rule has been adopted, compliance is over ninety-nine percent for citizens of the United States, Canada and Bermuda. The conclusion is that Americans and foreign nationals alike are willing to obtain the necessary documents to enter or re-enter the United States once the requirements are known and enforced. In short, more documentation and cross-cutting databases are in the future for border crossings; at the same

---

[99] *See supra* note 96.

[100] *Id.*

[101] American Civil Liberties Union, ACLU of Maryland Blasts New Real ID Regulations, *available at* http://www.aclu.org/privacy/gen/33952prs20080115.html http://www.aclu.org/privacy/gen/33952prs20080115.html (last visited Oct. 27, 2008). Needless to say a number of states have opted out of enforcing the ID.

[102] BBC News, Foreign National ID Card Unveiled, *available at* http://news.bbc.co.uk/2/hi/uk_news/politics/7634111.stm (last visited on Oct. 27, 2008).

time, any expectation of privacy or protection due to citizenship is severely diminished, if not extinguished. In the words of Stewart Baker, Assistant Secretary for Policy of the DHS, "[t]he development, production, and distribution of quality, physically secure documents, is an expensive process, as it requires replacing old document production systems and infrastructure; however, the investment will pay healthy dividends towards the security of this country."[103]

These programs flow from the 9/11 Report that recommended: 1) creating a strategy to combine terrorist intelligence, operations, and law enforcement; 2) integrating the U.S. border security system into a larger network of screening points; 3) implementing a biometric entry-exit screening system; and 4) enhancing international cooperation, particularly with Canada and Mexico.[104] The reason for the need of a technological web of connectivity recommended by the 9/11 Commission turns on the volume traffic and the size of the border. The United States has nearly 100,000 miles of shoreline and almost 6,000 miles of borders with its neighbors.[105] People and goods arrive daily at more than 3,700 terminals in 301 ports of entry.[106] To find "one man" amid the approximately 500 million people, 125 million vehicles and 21.4 million import shipments that came into the country last year, with 6 million cargo containers, 2.2 million rail cars and 11.2 million trucks "is about as likely as winning a lottery."[107]

The government's continuing commitment to win the lottery with border control and stem immigration is demonstrated by the 2007 Secure Border Initiative or SBInet which will deploy "a mix of personnel, technology, infrastructure

---

[103] Baker, *supra* note 97, at 5-6.

[104] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 385-90 (official gov't ed. 2004); *see also* YULE KIM, PROTECTING THE U.S. PERIMETER: "BORDER SEARCHES" UNDER THE FOURTH AMENDMENT 16 (CRS Report, Order Code RL 31826) (updated Jan. 15, 2008).

[105] Stephen E. Flynn, *Beyond Border Control*, 79 FOREIGN AFF. 57 (Nov./Dec. 2000).

[106] *Id.*

[107] *Id.*; *see also* Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1 (2003).

and response assets"[108] with a multi-billion dollar set of 300 miles of fencing and the potential for unmanned aerial vehicles patrolling the borders with high definition cameras currently deployed on the battlefields of Iraq and Afghanistan.[109] The goal is to create "smart borders" with electronic registration systems, visa programs and waiver systems for safe travelers.[110] It is estimated that there are between 11 and 12 million illegal immigrants in the United States. In early 2002, the Immigration and Naturalization Service director estimated that to control the border the department would need 27,000 investigators and special agents (at the time there were 2,000); 31,000 Border Patrol agents (in 2008 there are 18,000); 21,500 immigration inspectors (compared to 5,000); 15,600 deportation officers (compared to 650); 1,440 attorneys (compared to 777) and 110,000 detention beds (compared to 33,000 in 2008).[111] The cost and numbers are staggering. This confusion or clash of immigration policy with preventing terrorism underscores why the doctrines need to be thought through carefully and analytically, to truly create a "smart border."[112] Smart visa and passport tracking is essential since as pointed out by one of the more outstanding monographs produced by the 9/11 Commission, documentation was key to the attackers:

---

[108] *See* BLAS NUNEZ-NETO & YULE KIM, BORDER SECURITY: BARRIERS ALONG THE U.S. INTERNATIONAL BORDER 27-28 (CRS Report, Order Code RL 33659) (updated May 13, 2008). This report details the scores of acts that were waived by Congress to speed the construction of the San Diego fences and walls from the Federal Water Pollution Control Act to the Administrative Procedure Act. *Id.* at 47-48.

[109] JASON BLAZAKIS, BORDER SECURITY AND UNMANNED AERIAL VEHICLES 2 (CRS Report, Order Code RS 21698) (updated 2008).

[110] *See* Kenn Morris, *Moving Toward Smart Borders*, June 2003, *available at* http://www.sandiegodialogue.org/pdfs/Asa_Paper_June_03.pdf (last visited Nov. 28, 2008). Visa and tracking programs include: National Security Entry-Exit Registration System (NEERS), Student and Exchange Visitor System (SEVIS), etc.

[111] EDWARD ALDEN, THE CLOSING OF THE AMERICAN BORDER 297 (2008).

[112] *See* Susan Ginsburg, *Weaknesses In The Visa Waiver Program: Are The Needed Safeguards In Place To Protect America?*, Testimony Before the Senate Judiciary Committee, Subcommittee on Terrorism, Technology & Homeland Security (Feb. 28, 2008), *available at* http://www.homeland.ca.gov/pdf/testimony/senate/sju/02-28-08/Testimony_SusanGinsburg_TheMigrationPolicyInstitute.pdf (last visited Nov. 28, 2008).

> The success of the September 11 plot depended on the ability of the hijackers to obtain visas and pass an immigration and customs inspection in order to enter the United States. It also depended on their ability to remain here undetected while they worked out the operational details of the attack. If they had failed on either count—entering and becoming embedded—the plot could not have been executed.
>
> Here we present the facts and circumstances of the hijackers' travel operation, including their 25 contacts with consular officers and their 43 contacts with immigration and customs authorities. We also discuss the 12 contacts with border authorities by other September 11 conspirators who applied for a visa. The narrative is chronological, retracing the hijackers' steps from their initial applications for U.S. visas, through their entry into the United States, to their applications for immigration benefits, and up through their acquisition of state identifications that helped them board the planes. Along the way, we note relevant actions by U.S. government authorities to combat terrorism. There were a few lucky breaks for U.S. border authorities in this story. Mostly, though, it is a story of how 19 hijackers easily penetrated U.S. border security.[113]

Legal doctrine, however, in the border context continues to expand the use of new technology for state use. In 2007, the Director of National Intelligence designated DHS as the agent for the National Applications Office (NAO) to run satellite imagery over the United States.[114] A set of pre-9/11 Supreme Court cases explored imagery and the Fourth Amendment.[115] In *California v. Ciraolo*, the Court in a 5-4 decision held that warrantless aerial observation from 1,000 feet of a fenced-in-backyard containing marijuana did not constitute a search.[116]

---

[113] *See* Thomas R. Eldridge, Susan Ginsburg, Walter T. Hempel II, Janice L. Kephart, & Kelly Moore, *9/11 and Terrorist Travel*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *available at* http://govinfo.library.unt.edu/911/staff_statements/911_TerrTrav_Monograph.pdf (last visited Nov. 28, 2008).

[114] RICHARD A. BEST JR & JENNIFER K. ELSA, SATELLITE SURVEILLANCE: DOMESTIC ISSUES 7 (CRS Report, Order Code RL 34421) (updated on Mar. 21, 2008).

[115] *Id.* at 14-16.

[116] California v. Ciraolo, 476 U.S. 207 (1986).

On the same day, the Court also held in *Dow Chemical Co. v. United States* that aerial photography of an industrial compound from a greater altitude by government regulators, in navigable airspace using a specialized camera, was similarly not a search.[117] Some Justices on the Court, however, noted that if the compound had been a private home or the camera had been a unique sensory device able to penetrate the walls, a warrant might have been required.[118] Finally in *Florida v. Riley*, in a plurality opinion, the Court concluded that a police helicopter hovering at 400 feet in a surveillance flight observing through a greenhouse roof marijuana growing was not a Fourth Amendment violation.[119]

Naturally, in the context of the United States, using Department of Defense (DOD) assets such as satellite imagery raises potential violations of the Posse Comitatus Act.[120] In 1991, the Office of Legal Counsel in the Department of Justice opined, however, that the use of military personnel to conduct aerial infrared monitoring of private property for law enforcement purposes (assisting DEA in monitoring illicit narcotics production) was not a violation of the Posse Comitatus because the surveillance was not a search, seizure or arrest since there was no "physical contact" resulting in a direct confrontation between military and civilians.[121] Given the "border exception" and the "national security" considerations, the real questions for satellite imagery are not the constitutional ones — they appear to have been answered — but rather the policy ones posed by the report: How much "valued added" is satellite imagery? Is congressional oversight adequate? And, how does the government ensure that the NAO operates within the governing statutes for the intelligence agencies?[122] As in the

---

[117] Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[118] *Id.* at 237 n.4, 238. *See also id.* at 243 n.4 (Powell, J., dissenting).

[119] Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion).

[120] Posse Comitatus Act, 18 U.S.C. § 1385 (2008).

[121] Military Use of Infrared Radars Technology to Assist Civilian Law Enforcement Agencies, 15 U.S. Op. Off. Legal Counsel 36 (1991), *quoted in* BEST & ELSA, *supra* note 114, at 22-23.

[122] BEST & ELSA, *supra* note 114, at 25-26.

FISA example under the border exception cases, how does one monitor or maintain the US/non-US citizenship distinction on the border, "extended border" or "functional border" with satellite technology? The clash of doctrines at the border begin to converge as the power of technology allows for greater transparency by the state based on the threat of the individual at the price of immigration movements, privacy, autonomy and citizenship protections.

This quest and search of "actionable" intelligence, a smart border and the border exception has come together on laptop searches. In *United States v. Arnold*, the lower court in suppressing the evidence for trial found that "opening and viewing confidential computer files implicates dignity and privacy interests" and could not fall under the routine inspection border exception but required "reasonable suspicion."[123] Under the facts of the case, U.S. Customs and Border Patrol first questioned Arnold returning from the Philippines, booted up his computer, clicked on folders titled "Kodak Pictures" and "Kodak Memories" and found pictures of nude women.[124] Immigration and Customs Enforcement agents were then called in; they detained Arnold for several hours, continued to examine the computer and found what they believed to be child pornography.[125] The Court of Appeals in reversing the lower court's order to suppress the evidence re-emphasized the distinction the Supreme Court has established in its "border"

---

[123] United States v. Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal 2006).

[124] *Id.* at 1001.

[125] *Id.*

> A grand jury charged Arnold with: (1) "knowingly transport[ing] child pornography, as defined in [18 U.S.C. § 2256(8)(A)], in interstate and foreign commerce, by any means, including by computer, knowing that the images were child pornography"; (2) "knowingly possess[ing] a computer hard drive and compact discs which both contained more than one image of child pornography, as defined in [18 U.S.C. § 2256(8)(A)], that had been shipped and transported in inter-state and foreign commerce by any means, including by computer, knowing that the images were child pornography"; and (3) "knowingly and intentionally travel[ing] in foreign commerce and attempt[ing] to engage in illicit sexual conduct, as defined in [18 U.S.C. § 2423(f)], in a foreign place, namely, the Philippines, with a person under 18 years of age, in violation of [18 U.S.C. § 2423(c)]."
>
> United States v. Arnold, 523 F.3d 941, 943 (9th Cir. 2008).

jurisprudence of "particularized suspicion" between searches of the "person" versus those involving "property."[126] The appellate court reasoned that computers are more like vehicles or property than objects with special "privacy interests" that would trigger an "intrusiveness analysis" of the person as in a body cavity search.[127] The appellate court went on to note that the Supreme Court's other two narrow exceptions to a search, when "exceptional damage to the property" had taken place or when the search was "particularly offensive," had not been triggered by the mere booting up the computer.[128] The court further rejected any claim that the computer could be thought of as "capable of functioning as a home" for a Fourth Amendment analogy.[129] Finally, the court approvingly cited a Fourth Circuit case, *United States v. Ickes*, in which the defendant's van was searched and a video camera containing a tennis match that "focused excessively on a young ball boy" prompted a more thorough examination of the van where more prepubescent pornography was uncovered.[130] The Fourth Circuit rejected any First Amendment defense in the *Ickes* case, particularly given the threat of terrorism.[131] The *Arnold* court was persuaded by the analysis and followed its reasoning:

> The Fourth Circuit held that the warrantless search of defendant's van was permissible under the border search doctrine. The court refused to carve out a First Amendment exception to that doctrine because such a rule would: (1) protect terrorist communications "which are inherently 'expressive'"; (2) create an unworkable standard for government agents who "would have to decide—on their feet—which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First

---

[126] *Arnold*, 523 F.3d at 945-46.

[127] *Id.* at 946.

[128] *Id.*

[129] *Id.* at 947.

[130] *Id.* at 948.

[131] *Id.*

> Amendment interest is also at stake. *See id.* at 506-08 (citing *New York v. P.J. Video*, 475 U.S. 868, 874 (1986) (refusing to require a higher standard of probable cause for warrant applications when expressive material is involved)).[132]

One can hear the doctrines locking into place or clashing, depending on one's view. The computer has become a "digital briefcase" of the twenty-first century.[133] This concern is reflected in an earlier Ninth Circuit case, *United States v. Romm*,[134] however there the court never discussed the routine versus non-routine nature of the computer search where the search included a computer forensic team that was able to recover deleted files and determine when the files were created, opened, or modified.[135] As speculated by one commentator, consider someone receiving an unsolicited, spam e-mailing containing illicit photos.[136] Even if deleted, a border search might reveal the message and it could be used against the individual in court, given the recent *Arnold* decision.[137]

As one would expect, speculation soon became reality; given technology, the border exception, and one's expectation of privacy, it was only a matter of time before a case arose. The next legal doctrine to be brought into play by the border jurisprudence is the Fifth Amendment, or the right against self-incrimination. Thus far, the closest case on point is *In Re*

---

[132] *Id.*

[133] *See* Michael Pellegrino, *International Business Travelers Beware*, ILL BUS L.J. (Feb. 22, 2008), *available at* http://iblsjournal.typepad.com/illinois_business_law_soc/2008/02/picture-yoursel.html (last visited Nov. 28, 2008).

[134] United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

[135] *Id.* at 994-95.

[136] *See* Pellegrino, *supra* note 133.

[137] *See Arnold*, 523 F.3d at 947. The *Arnold* holding rejects the view that a search of a person's laptop implicates privacy and dignity interests. *Id.* In an earlier case, *United State v. Molina-Tarazon*, it was asserted that "government intrusions into the mind . . . are no less deserving of Fourth Amendment scrutiny than [physical intrusions]." 279 F.3d 709, 716 (9th Cir. 2002). The *Molina-Tarazon* court indicated that because of the vast amount of private thoughts and sensitive data that can be stored on data drives, searching them is analogous to searching the mind, and thus they implicate privacy and dignity interests. *Id.* at 716. Consequently, the court held searches of laptops and other electronic storage devices require reasonable suspicion. *Id.* at 717.

Boucher.[138] Sebastien Boucher was crossing the border from Canada to Vermont when border agents began to question him.[139] Agents saw a laptop in the back seat of his car and opened it up.[140] His computer was not password-protected; an agent began to look through it.[141] The agent came across 40,000 image files with titles that strongly suggested the files themselves were child pornography.[142] For example, one file was labeled "2yo getting raped during a diaper change."[143] The files had been opened six days earlier, but the agent found that he could not open the file when he tried to do so.[144] Agents asked Boucher if there was child pornography in the computer, and Boucher said that he was not sure.[145] He downloaded a lot of pornography onto his computer, he said, but he deleted child pornography when he came across it.[146] Boucher then assisted the officer in accessing drive Z that contained preteen pornography.[147] The computer was seized and the agents made a mirror image of the drive, but when they tried to access the Z drive again, it was protected by "Pretty Good Privacy" (PGP) software, which encrypted, password-protected the material, and made it inaccessible.[148] A grand jury subpoenaed the password and Boucher pled the Fifth.[149]

Though both the government and Boucher agreed the "contents" of the computer were not protected by the Fifth Amendment, Boucher argued the "password" was testimonial, protected and privileged.[150] Fingerprints, blood samples and

---

[138] *In Re Boucher*, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).
[139] *Id.* at *1.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.* at *2.
[148] *Id.*
[149] *Id.*
[150] *Id.*

voice recording are not protected under the Fifth Amendment.[151] As noted by the court in *Boucher,* the Supreme Court in *United States v. Hubbell*[152] reasoned that while a combination to a wall safe was testimonial and protected, surrendering a key to a strongbox was not.[153] The magistrate judge, Jerome J. Niedermeier, found that a password is more like a combination, since it is in the suspect's mind, it is not a "physical thing," it compels him to display the contents of his mind, and therefore must be protected:

> Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" If Boucher does know the password, he would be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court.[154]

Critics of the case note that the government already knew that the files belonged to Boucher since the computer was in his car; the government was aware that he knew the relevant password partly because he assisted them in searching the Z drive; and Boucher admitted to downloading material during the interview.[155] Therefore, the alleged self-incrimination that follows from Boucher's revealing his password is simply the content of these other accessible computer files.[156] The government will not be forcing the defendant to let the officers know that he is linked to the computer files, the evidence will instead be the product of lawful investigation followed by a demand for a password that everyone already knew the

---

[151] *Id.* at *4.

[152] United States v. Hubbell, 530 U.S. 27, 43 (2000).

[153] *In Re Boucher*, 2007 WL 4246473 at *4.

[154] *Id.* at *4.

[155] *See* Sherry F. Colb, *Does the Fifth Amendment Protect the Refusal to Reveal Computer Passwords? In a Dubious Ruling, A Vermont Magistrate Judge Says Yes*, (Feb. 4, 2008), *available at* http://writ.news.findlaw.com/colb/20080204.html (last visited Nov. 28, 2008).

[156] *Id.*

defendant possessed.[157] What the defendant had to do, in other words, was surrender a password much like a key to a briefcase or a locked compartment inside a trunk. Under the critics' analysis the government could grant immunity for the password and then prosecute for the underlying contents of the files, and a refusal to provide the password would amount to contempt and possible incarceration.[158]

These facts are underscored by the Office of National Counterintelligence Executive's warning for those traveling abroad and what one can expect to encounter at border crossings. But in the *Boucher* case rather than national security issues it appears that criminal activity is what is at stake. Though Fourth Amendment protection is diminished at the border, for U.S. citizens in a non-national security case, is similarly the Fifth Amendment? Clearly one could not take a briefcase across the border and refuse to have its contents examined. Is a computer a digital briefcase without Fifth Amendment protection? Eventually the Supreme Court will have to address this question and resolve the clash of these doctrines—maybe.

III. CONCLUSION: TRADE-OFFS, BALANCING OR RESILIENCY?

Combating terrorism in the digital age has produced a clash of legal, political and social doctrines. Technology, theories of state power, the individualized nature of modern terrorism, and our legal traditions have clashed over the need for security. A threshold question for the public policy debate is whether or not one believes the threat of terrorism is an *existential* threat. For some, an existential threat is one that can only be posed by a competing state power with nuclear weapons; terrorism therefore is not such a threat. Terrorism is a form of "empire baiting" and must be countered with measured law enforcement approaches that respect our legal traditions and follow our civil

---

[157] *Id.*

[158] Declan McCullagh, *Judge: Man can't be forced to divulge encryption passphrase*, (Dec. 14, 2007), *available at* http://news.cnet.com/8301-13578_3-9834495-38.html (last visited Nov. 28, 2008).

liberties. Any intrusive government measure must be balanced against how our freedoms or rights are diminished. This approach is more willing to accept risk at the expense of faux security since stopping all attacks is impossible. Additionally, this approach advocates more focus on resiliency, building infrastructure and redundancy in our system.

For others, a terrorist with one nuclear device or biological weapon poses a threat that justifies expansive executive powers and enhanced investigative tools to prevent any and all attacks, the key to prevention. Security or the chance to stop a terrorist is worth the diminution of certain rights or privileges. For this school of public policy, our security forces our people of good will who are making sacrifices to protect the republic: only those who have something to hide—terrorists, criminals and violators—should fear this new requirement of personal transparency. Government violations or infractions will be on the margin and prosecuted accordingly.

For those in the legal arena the clash becomes focused on specific cases involving specific property, or persons at specific locations—borders and computers—triggering specific articles and clauses of the Constitution—the Fourth Amendment, the Fifth Amendment, and separation of powers. As de Tocqueville pointed out in the early nineteenth century in *Democracy in America*, "[s]carcely any political question arises in the United States that is not resolved, sooner or later, into a judicial question."[159] The legal balancing requires an analysis of the inherent power of the President, congressional statutes and the power of particular rights in the context of the threat, since no right is absolute.

The Supreme Court jurisprudence in this area has shown significant deference to the sovereignty of the state to defend its territory at the diminution of Fourth Amendment protection. U.S. citizens and non-U.S. citizen travelers are treated alike and receive minimum protection when at the border. Computer technology and encryption are raising Fifth Amendment rights

---

[159] 1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA, 280 (Phillips Bradley, ed., Alfred A. Knopf 1948) (1945).

in the face of states need to gather information for criminal and terrorist networking at ports of entry. Eventually the Court will be called on to balance these interests. The Court's border jurisprudence currently leans towards the state's need to protect.

Similarly, foreign borders, as the NCIX has warned, are potential Wild West frontiers whereby electronic data can be mirrored and monitored for the foreign state's advantage. The electronic frontier, from the perspective of the individual or business entity, is currently a hostile environment due to the state's fear of the potential for individualized attack and the state's need for critical information for advantage. The current jurisprudence has not been a safe port in the storm.

In the opening quotation of this article, Senator Feingold reasoned, "if the courts can't offer that protection, then that responsibility falls to the Congress."[160] Yet, Congress thus far has not legislated on border cases, and its performance in the FISA area has not satisfied too many: More study is required.[161]

---

[160] *See supra* note 1 and accompanying text.

[161] *See Restoring the Rule of Law: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary* (2008), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3550&wit_id7415 (last visited Nov. 28, 2008) (testimony of Suzanne E. Spaulding, Principal, Bingham Consulting Group LLC). Spaulding suggests that the new administration should conduct a comprehensive review of domestic spying. *Id.* Some of the key issues that any comprehensive review should address include:

- A review of the Foreign Intelligence Surveillance Act, including changes enacted as part of the PATRIOT Act and in the amendments this summer, assessing both the statutory language and its implementation.
- The recent amendments focused on meeting a particular need asserted by the current Administration and, as noted earlier, many Member of Congress stated their view that it was a deeply flawed bill and should be re-visited in the coming session of Congress. Beyond that, however, what seemed lost in the debate is the need to reassess FISA more generally in light of the vastly higher level of international communications engaged in by Americans today, via the Internet as well as by phone, than was the case in 1978. Does it still adequately protect innocent Americans from unwarranted government intrusion into their private communications?
- In addition, the electronic and physical search provisions of FISA, complex from their inception, have become virtually impenetrable to nearly all but those who work with it on a daily basis—and perhaps even to those unfortunate souls! Is

Moreover, immigration law and anti-terrorist measures have become so entangled that America's historic ability to be a beacon for the world's talent has been called into question over our administration of the skilled visa program.[162]

The clash of doctrines has been a function of the difficulty of the problem set. Each institution, the executive, the legislature and the courts, has approached the interlocking propositions sketched out at the beginning of the article from each of its institutional competencies. The results thus far have been unsatisfactory from all policy perspectives. Science and technology have been the key engines to our prosperity and quality of life; while at the same time these disciplines have produced the existential threats that can end both.

The executive, the congress and the courts, are at the beginning of the regime of how to combat terrorism in the digital age. There is a clear need to forge new principles and norms to harmonize the din that is resulting from the clash.[163] More institutional reform is needed for the Intelligence Community (IC) and the law enforcement community. The creation of the

---

there a way to simplify this regime to ensure compliance, enhance the prospects for effective oversight, and improve public trust?

- This review should include careful consideration of the important role of judges. As Supreme Court Justice Powell wrote for the majority in the Keith case:

> The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Id. at 4.

[162] See discussion of H1-B visas for skilled workers, whereby Microsoft was unable to acquire visas for a third of the foreign job candidates it required. EDWARD ALDEN, THE CLOSING OF THE AMERICAN BORDER: TERRORISM, IMMIGRATION AND SECURITY SINCE 9/11, 282 (2008).

[163] Concluding paragraphs drawn from Harvey Rishikof, *The "War on Terror" and Prevention: Improving the Domestic Paradigm for the Digital Age*, 17 THE NAT'L STRATEGY FORUM REV. 1, *available at* http://www.nationalstrategy.com/Programs/NationalStrategyForumReview/PastNSFRIssues/Winter2007NSFRV171/tabid/112/Default.aspx (last visited Nov. 28, 2008).

Director of National Intelligence has not resulted in the coordination for which many had hoped. The need for better collection, analysis and dissemination of information still plagues the IC. In addition, better delineation of the role of military intelligence and its relation to its civilian counterparts requires more analysis and connectivity. A National Commission is required to draw on expertise from both sides of the political aisle, the private sector and the legal defense bar to craft a long-term reform package to balance the equities of the parties involved in prosecuting the War on Terror.

Second, the debate over executive authority and congressional reticence must come to an end. The assertions of presidential authority excluding Congress and barring Congress from helping to shape and structure surveillance programs have helped generate unnecessary suspicion and rancor. A way must be fashioned to generate a better working relationship between Congress and the Oval Office. There must be adequate due process protections built into reforms to satisfy traditional concerns of privacy, the current FISA reforms need to be revisited.

Third, the judiciary must be part of the review process whenever surveillance of U.S. or non-U.S. parties is involved. As the government increasingly relies on the private sector to gather data, and then uses this data forever increasing sophisticated data mining, judicial supervision should be part of the process. As more intrusive technological tools become available, reform packages must include more resources for robust Inspector General investigations. Current border jurisprudence enhances the need for a national security court with expedited procedures for review and concentrated expertise in due process, as had been done in civil law countries.[164]

Fourth, given the nature of globalization, the digital world and borders, a more international approach is required to address the issues. This enterprise will have to address the

---

[164] *See* Harvey Rishikof, A FEDERAL TERRORISM COURT, PPI, Nov. 14, 2007, *available at* http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecID=307&contentID=254507 (last visited Nov. 28, 2008).

issue of *Weberian* sovereignty head on. What are the limits to the State's ability to have access to electronic data, and what will be the international penalties for violating such norms? This is a tough issue, but avoidance is not the answer.

This will be the challenge for our generation, but it is a challenge we must meet because too much is at stake. How we treat borders and data will define the power of the state and privacy in the twenty-first century.

The James Otis Lectures

ANNUAL LECTURE SERIES

This lecture series is fittingly named after the man who not only ignited the American Revolution, but whose very words in opposition to the writs of assistance inspired the Fourth Amendment, James Otis.

Born in Great Marshes (now West Barnstable), Massachusetts, the eldest of thirteen children, Otis would devote his life to the law, as his father and grandfather had done before, becoming one of the most revered trial advocates and legal orators throughout Massachusetts, earning him the coveted position as Advocate General of the Vice-Admiralty Court at just thirty-one years of age, a position he would later resign to champion the cause against the Crown's arbitrary issuance of writs of assistance. The writs were general search warrants that permitted the authorities to search anywhere they pleased for any reason—or for no reason. In one of the first defiant stands against British authority in the Colonies, Otis attacked the writs as

"'against the fundamental principles of law.'"[1] He asserted, among other things: "A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege."[2]

John Adams, who witnessed Otis's impassioned oration, afterward declared: "Every man of an [immense] crowded audience appeared to me to go away, as I did, ready to take arms against [Writs] of Assistance. Then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[3]

Although Otis may have lost his case before the Massachusetts Superior Court in Boston's Old Town Hall that day, he gained a place in history. In that case, "the American tradition of constitutional hostility to general powers of search first found articulate expression."[4] It was Adams, so inspired by Otis's words, who later drafted Article Fourteen of the Massachusetts Declaration of Rights of 1780, which served as the model for the Fourth Amendment.

Otis would become one of the greatest Patriots our country has ever known. Though eventually reduced to insanity and ultimately silenced by a bolt of lightning, James Otis will forever remain first among America's Fourth Amendment advocates.

Thomas K. Clancy[*]

---

[1] TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 36-37 (1969) (quoting 2 LEGAL PAPERS OF JOHN ADAMS 125 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

[2] *Id.* at 37 (quoting 2 LEGAL PAPERS OF JOHN ADAMS, *supra* note 1, at 142).

[3] 2 LEGAL PAPERS OF JOHN ADAMS, *supra* note 1, at 107.

[4] M.H. SMITH, THE WRITS OF ASSISTANCE CASE 7 (1978).

[*] Director, National Center for Justice and the Rule of Law. The Center, and consequently this lecture series and articles stemming from it, is supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles are those of the author and do not represent the official position of the United States Department of Justice.

ENVISIONING POST-CONVICTION REVIEW FOR THE TWENTY-FIRST CENTURY

Nancy J. King[1] *& Joseph L. Hoffmann*[2]

This lecture poses the following question: What would happen if we radically rethought our approach to post-conviction review? Our present system of post-conviction review has outlived its utility. New empirical research reveals that the system wastes scarce resources and produces very little tangible benefit. Drawing on several discrete ideas that others have advanced before, and adding a few new ones, we can begin to sketch out a new model for post-conviction review tailored to the needs and circumstances of criminal justice today.[3]

I. THE PROBLEM

The present system of review for state criminal judgments has been in place since about the mid-1960s or so. It involves multiple, often duplicative stages: (1) a direct appeal, which can include multiple proceedings in several different courts that are all considering the same questions; (2) state post-conviction

---

[1] Speir Professor of Law, Vanderbilt University. Professor King delivered this 2008 Otis Lecture in April 2008 based on ideas she and Professor Hoffmann worked out together. The first person—"I"—thus refers to Professor King, and "we" indicates both authors.

[2] Harry Pratter Professor of Law, Indiana University School of Law - Bloomington.

[3] This lecture presents our initial outline of a preliminary idea that is developed and significantly changed in a later article, *Rethinking the Federal Role in State Criminal Justice*, forthcoming in 84 N.Y.U. L. Rev. (2009).

proceedings, where again, the same questions may be considered several times by several different courts; and (3) federal habeas corpus review, where constitutional questions are raised in the district court, then in the federal court of appeals, and often in yet another certiorari petition to the U.S. Supreme Court.

This system was created to cope with a revolution in the regulation of the criminal process—the incorporation of the protections in the Bill of Rights against the states through the Fourteenth Amendment's Due Process Clause. In 1950 relatively few state prisoners would have been able to seek relief in federal court because the Due Process Clause had been interpreted to protect against only those actions by states that infringed fundamental fairness; many of the criminal procedure protections enjoyed by federal defendants had been denied to state defendants.[4] Then, in a series of cases decided over twenty years, the Court simultaneously expanded both the reach of federal law and its enforcement in federal court. By the mid 1970s, the Court had extended to state prisoners dozens of new constitutional claims[5] and a wide-open invitation to raise them before federal judges.[6] To fend off federal interference and provide their own review, states responded by creating post-conviction mechanisms of their own that a prisoner must navigate before heading to federal court.[7]

Why rethink this system now? Because it has outgrown its usefulness. Rights have continued to expand, while prison populations and average terms served[8] have grown even faster.[9]

---

[4] *See generally* 1 WAYNE LAFAVE, JEROLD ISRAEL, NANCY KING & ORIN KERR, CRIMINAL PROCEDURE § 2.4 (3d ed. 2007); *see also id.* at § 2.6(b) n.34 (collecting cases in which the Court extended a criminal procedure guarantee to state defendants in the 1960s and overruled precedent from the 1930s and '40s).

[5] *Id.*

[6] For a discussion of the expansion of habeas corpus review from "jurisdictional" error to constitutional violations, see LAFAVE ET AL., *supra* note 4, at § 28.3(b).

[7] *See* 1 DONALD E. WILKES, JR., STATE POST-CONVICTION REMEDIES AND RELIEF HANDBOOK WITH FORMS § 2:5 (2007-08) (noting the expansion of criminal procedure rights and habeas review "put pressure on and also encouraged the states to upgrade the quality of their postconviction relief machinery").

[8] BUREAU OF JUSTICE STATISTICS, SOURCEBOOK OF CRIMINAL JUSTICE STATISTICS 511 tbl.6.44 (Ann L. Pastore & Kathleen Maguire, eds., 2003) (finding that, excluding life sentences, the average time served jumped seven months for first releases from state

We think that the cost of this multi-layered review system has far surpassed its benefits, at least in all but the relatively small number of cases that involve the death penalty. The Constitution would be better served by abandoning the effort to prop up the complex remedial system that state and federal courts are struggling to provide long after conviction and shifting those resources into indigent criminal defense earlier in the process.

A. Wasted Effort on the Backend

This country has the highest imprisonment rate in the world.[10] Among the many consequences of this dubious distinction is the record number of petitions that prisoners file each year in federal and state court seeking relief from convictions and sentences. This litigation consumes an enormous amount of taxpayer dollars.[11]

In 1996, Congress passed a law—the Anti-Terrorism and Effective Death Penalty Act ("AEDPA")[12]—in an effort to streamline federal habeas review of state criminal judgments and reduce post-conviction litigation costs in federal courts.[13]

---

prison between 1990 and 1999, and the percentage of sentence served increased from thirty-eight to forty-nine percent); PAULA M. DITTON & DORIS JAMES WILSON, BUREAU OF JUSTICE STATISTICS, SPECIAL REPORT: TRUTH IN SENTENCING IN STATE PRISONS 7–9 (1999).

[9] BUREAU OF JUSTICE STATISTICS, *supra* note 8, tbl.6.29.2006 (showing that nationwide, the number of state prisoners per 100,000 population doubled from 130 in 1980 to 272 in 1990, then nearly doubled again to 445 by 2006); *id.* tbl.6.28.2006.

[10] International Centre for Prison Studies, Prison Brief for United States of America, http://www.kcl.ac.uk/depsta/law/research/icps/worldbrief/ (follow "North America" hyperlink; then follow "United States of America" hyperlink) (last visited Oct. 17, 2008) (noting that the United States has an imprisonment rate of 7,621 per 100,000 population).

[11] Both state and federal courts have seen an increase in post-conviction filings. *See, e.g., Growing Number of Inmates Turning to Post-Conviction Relief*, NEWSDAY, Sept. 10, 2006 (the number of cases growing 46 percent over the past four years); source cited *infra* note 14.

[12] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of 8, 18, 22, 28, 40, and 42 U.S.C.).

[13] *E.g.*, Crouch v. Norris, 251 F.3d 720, 724 (8th Cir. 2001) ("The scant legislative history discussing the purpose of AEDPA's habeas restrictions indicates that Congress was concerned with delay and finality").

Last fall, together with researchers at the National Center for State Courts and with funding from the Department of Justice, I completed the first empirical study of habeas litigation after AEDPA.[14] The study examined separate samples of capital and non-capital state prisoner filings in habeas, but the focus here is on the non-capital cases. Over 18,000 federal habeas cases are filed each year by state prisoners.[15] The sample examined in the study was a random sample of all non-capital habeas cases filed by state prisoners nationwide.[16] We found that not only are these cases taking a long time to process—longer than before AEDPA[17]—but also that the vast majority of the time, energy, and money spent on federal habeas is wasted. Federal habeas is essentially a futile exercise for state prisoners serving non-capital sentences.

In the first place, federal review is essentially out of reach to most prisoners. Only those with particularly long sentences have meaningful access. The study showed that state prisoners take on average at least five years to reach federal court.[18] This rules out access to habeas review for most people convicted of felonies in state court, sixty percent of whom don't go to prison

---

[14] NANCY J. KING, FRED L. CHEESMAN II & BRIAN J. OSTROM, FINAL TECHNICAL REPORT: HABEAS LITIGATION IN U.S. DISTRICT COURTS 26 (2007), http://www.ncjrs.gov/pdffiles1/nij/grants/219559.pdf (hereinafter HABEAS STUDY).

[15] FRED L. CHEESMAN, II ET AL., NAT'L CTR. FOR STATE COURTS, A TALE OF TWO LAWS REVISITED: INVESTIGATING THE IMPACT OF THE PRISONER LITIGATION REFORM ACT AND THE ANTITERRORISM AND EFFECTIVE DEATH PENALTY ACT (2004), http://www.ncsonline.org/WC/Publications/Res_PreCiv_TwoLawsRevPub.pdf; JAMES C. DUFF, ADMINISTRATIVE OFFICE OF THE U.S. COURT, JUDICIAL BUSINESS OF THE U.S. COURTS 90-94 tbl.B-1A,145-47 tbl.C-2, http://www.uscourts.gov/judbus2007/contents.html.

[16] HABEAS STUDY, *supra* note 14, at 15-16.

[17] *Id.* at 56, 59 (median processing time for completed cases increased from 6 to 7.1 months; taking into account cases still pending, average processing time was over a year). For pre-AEDPA statistics, see ROGER A. HANSON & HENRY W.K. DALEY, FEDERAL BUREAU OF JUSTICE STATISTICS, HABEAS CORPUS REVIEW: CHALLENGING STATE COURT CRIMINAL CONVICTIONS (1995), http://www.ojp.usdoj.gov/bjs/pub/pdf/fhcrcscc.pdf; Victor E. Flango & Patricia McKenna, *Federal Habeas Corpus Review of State Court Convictions*, 31 CAL. W. L. REV. 327 (1995).

[18] HABEAS STUDY, supra notes 14, 55-56 (noting the average filing period is 5.1 years excluding cases challenging administrative decisions and excluding cases found to be time barred; average filing period for all cases was over six years). This actually is longer after AEDPA's statute of limitations than it was before. *Id.*

at all.[19] The median sentence of those that do receive prison time is less than three years,[20] so most state prisoners are no longer incarcerated by the time they are in a position to file a federal petition. Not surprisingly, the study found that only twelve percent of noncapital habeas were filed by prisoners with a sentence of five years or less,[21] while nearly thirty percent were filed by prisoners serving life sentences, even though lifers make up fewer than two percent of people in prison.[22] In short, for most of those who enter state prisons, the Great Writ is inaccessible.

Secondly, even those that *do* reach federal habeas court don't get relief. Federal judges deny or dismiss almost every petition that is filed. In our sample, only seven petitioners (out of nearly 2,400) received any sort of relief (and at least one of these has already been overturned on appeal).[23] That is a one third of one percent chance the prisoner will succeed in getting an order to be retried, resentenced, or else released. These cases represent a substantial drain on the limited resources of the American criminal justice system for almost no return. Another important cost, albeit an indirect one, is the likelihood that meritorious claims of error will get lost or overlooked in the constant barrage of meritless claims.

B. Missed Opportunities at the Front End

Not only do we spend far too much on futile, successive post-conviction proceedings, but we spend these scarce resources in the wrong place. The cost of post-conviction review squanders state and federal criminal justice dollars, instead of spending them where they are needed most. Forty years after the Court announced the right to counsel in state criminal proceedings in

---

[19] MATTHEW DUROSE & PATRICK LANGAN, BUREAU OF JUSTICE STATISTICS, FELONY SENTENCES IN STATE COURTS, 2004 (2007), http://www.ojp.usdoj.gov/bjs/pub/pdf/fssc04.pdf.

[20] *Id.*

[21] HABEAS STUDY, *supra* note 14, at 20.

[22] *Id.* at 20, 54; DUROSE & LANGAN, *supra* note 19.

[23] HABEAS STUDY, *supra* note 14, at 52.

Gideon v. Wainwright,[24] and nearly twenty-five years after the Court outlined the test a prisoner must meet in order to receive relief for errors of his counsel in *Strickland v. Washington*,[25] inadequate indigent defense remains the most pressing challenge affecting constitutional rights in criminal justice today. Lack of training and experience, heavy caseloads, low pay, and little funding for investigation continue to plague defense services in state criminal cases.[26]

Because defense lawyers must preserve issues for review, the crisis in indigent defense at the trial and appellate levels is directly related to the wastefulness of post-conviction proceedings. The mistakes of counsel show up as procedural defaults—forfeitures of claims that were never raised when and where they should have been. Post-conviction litigation too often focuses on these forfeitures and whether they should be excused instead of on the merits of constitutional claims.

Twenty-five years of enforcing *Strickland* has not improved the situation. At one time, some may have hoped that it would have. In practice, however, relief under *Strickland* remains essentially hypothetical in non-capital cases. It is available only if the defendant (1) does not waive through his plea the right to raise a *Strickland* claim in post-conviction review,[27] (2) is sentenced long enough to reach a post-conviction stage where a record can be made, [28] (3) can show that his lawyer's action was

---

[24] 372 U.S. 335 (1963)

[25] 466 U.S. 668 (1984).

[26] *See, e.g.*, AMERICAN BAR ASSOCIATION'S STANDING COMMITTEE ON LEGAL AID AND INDIGENT DEFENDANTS, GIDEON'S BROKEN PROMISE: AMERICA'S CONTINUING QUEST FOR EQUAL JUSTICE (2004), http://www.abanet.org/legalservices/sclaid/defender/brokenpromise/fullreport.pdf; Bryan A. Stevenson, *Confronting Mass Imprisonment and Restoring Fairness to Collateral Review of Criminal Cases*, 41 HARV. C.R.-C.L. L. REV. 339, 342-45 (2006) ("States are unable to fund adequate indigent defense systems or provide sufficient resources for oversight, training, and management of cases.").

[27] *See* Douglas A. Morris, *Waiving an Ineffective Assistance of Counsel Claim: An Ethical Conundrum*, 27 CHAMPION 34 (2003) (noting the increasing use of such waivers by federal prosecutors, and arguing that defendants should require the advice of independent counsel in order to make them).

[28] The complaints about the futility of ineffectiveness litigation are not new. Professor Eve Brensike Primus argued last year in the Cornell Law review that

not strategic, and, hardest of all, (4) can show a reasonable probability of a different outcome had the error never happened.[29] And because even winning a *Strickland* claim carries no consequence for those providing representation, its deterrent power is practically nil.[30]

Anyone involved in the criminal justice system for very long will have a story to tell about oversights of defense attorneys at the trial or appellate level that *Strickland* could not correct. One particularly egregious example is described by Professor Jon Gould, Chair of the Innocence Commission for Virginia, in his new book *The Innocence Commission*.[31] The case involved a lawyer who both failed to cross-examine the detective who presented the defendant's confession and failed to check whether his client's blood, semen, and prints matched what the police had found during the investigation.[32] The defendant was convicted of rape, and he later alleged in post-conviction proceedings that he had received ineffective assistance of counsel. *Strickland* proved utterly useless. The federal courts reviewing his case found that because of the overwhelming evidence of guilt, including his confession, the defendant could not demonstrate adequate "prejudice" from his attorney's incompetence, which is the showing required for relief under *Strickland*.[33] Years later, the defendant was exonerated by DNA tests, and even won a civil judgment against the detective

---

ineffective assistance of counsel ("IAC") claims are out of reach for most defendants so long as they are relegated to state post-conviction proceedings years after conviction. Eve Brensike Primus, *Structural Reform in Criminal Defense: Relocating Ineffective Assistance of Counsel Claims*, 92 CORNELL L. REV. 679 (2007).

[29] Strickland v. Washington, 466 U.S. 668, 694 (1984).

[30] For commentary on the anemic regulatory effect of *Strickland* litigation, at least in non-capital cases, see Primus, *supra* note 27, at 688-97.

[31] JON B. GOULD, THE INNOCENCE COMMISSION: PREVENTING WRONGFUL CONVICTIONS AND RESTORING THE CRIMINAL JUSTICE SYSTEM 79-83 (2008).

[32] *Id.* at 170. In another case, a defendant was convicted of rape even though he testified at trial that he had had a vasectomy and thus could not have been the source of the sperm found in the victim. The medical records proving the defendant's vasectomy prior to the rape were never obtained by defense counsel, and the defendant remained imprisoned for ten years until DNA, and those medical records, exonerated him. *Id.* at 169-70.

[33] *Id.* at 81.

who had pressured him to confess to a crime he never committed.

The statistics from the recent study of habeas cases confirm what a waste of resources *Strickland* claims presently entail, at least for non-capital prisoners seeking relief in federal court. Although half of the non-capital cases in the study raised a claim of ineffective assistance,[34] in only one case out of nearly 2,400 was relief granted, and that grant was later overturned on appeal.[35] Nearly twenty percent of the non-capital cases filed involved a procedurally defaulted claim,[36] but in none did a federal court grant relief after concluding that a procedural default should be forgiven because of the denial of effective counsel.[37]

II. RESPONDING TO THE PROBLEM

A. Doomed Strategies for Repair

Many maintain that the problems with futility at the post-conviction stage can be traced to the restrictions on access to post-conviction relief and the refusal to provide lawyers after direct appeal. They argue, in other words, that relief is rare not because there are so few meritorious claims but because so many meritorious claims are never raised or, if raised, never remedied.[38] Put differently, the rare habeas grant is not a needle in a haystack; it is the tip of an iceberg.

Some who share this view believe the solution is obvious: add lawyers to post-conviction phases;[39] repeal the restrictions

---

[34] HABEAS STUDY, *supra* note 14, at 28.

[35] *Id.* at 52, 116.

[36] *Id.* at 48. The failure of prisoners to secure adequate legal advice also contributes to the remarkably high proportion of federal petitions by non-capital prisoners that are dismissed as time barred—more than one in every five petitions. *Id.* at 46.

[37] *Id.* at 115-16.

[38] *See, e.g.*, Stevenson, *supra* note 25; Larry W. Yackle, *State Convicts and Federal Courts: Reopening the Habeas Corpus Debate*, 91 CORNELL L. REV. 541 (2006); Roger Berkowitz, *Error-Centricity, Habeas Corpus and The Rule of Law as The Law of Rulings*, 64 LA. L. REV. 477 (2004).

[39] Stevenson, *supra* note 25, at 358.

in AEDPA;[40] beef up the *Strickland* test so that it is easier to meet;[41] and, as one professor recently proposed, overrule *Stone v. Powell* and consider Fourth Amendment claims on habeas.[42]

We believe that this is exactly the wrong response. Without speedier access to these phases of post-conviction review, making these phases more defendant-friendly would benefit only those sentenced to the longest sentences. Moreover, the extra strain these reforms would place on state resources would make review even more unobtainable for everyone else. Even for the small portion of inmates who actually receive post-conviction review, a lawyer is useless without better representation at the trial level to preserve objections to error. Lawyers at the back end can do very little to remedy claims of error which have been defaulted back at trial or on appeal.

B. A New Way: The Trade-Off

We propose a very different approach to thinking about the future of post-conviction review. In our view, the starting point must be the recognition that the two problems discussed above—the wasteful efforts *after* direct appeal and the continued deficiencies in the provision of adequate counsel *before and during* appeal—are joined at the hip. Changes in one can and should be linked to changes in the other. What is needed is a solution that would allow the states to shift dollars that they now waste at the back end forward to trial and appeal at the front end, where those resources can make the kind of meaningful difference for the accused that *Strickland* and post-conviction review never could. Even if federal habeas cannot be repaired as a reliable means of error correction for most prisoners, if recast it can serve a useful role as a political and economic incentive to encourage the states to provide a reliable means of error prevention.

Implementing this idea would probably require Congress to

---

[40] *Id.* at 358-59.

[41] Yackle, *supra* note 37, at 567.

[42] *See* Steve Semeraro, *Enforcing Fourth Amendment Rights Through Federal Habeas Corpus*, 34 SEARCH & SEIZURE L. REP. 49 (2007)

amend the habeas statute to provide a quid pro quo.[43] If a state takes specified steps to effectively reform its system of defense representation at the trial and appellate level, then federal habeas review could be scaled back drastically from what it is today, and federal funds would be made available to assist in maintaining adequate defense representation. Conversely, if a state fails to implement front-end reforms, existing habeas review could be expanded (for example, by returning to the "deliberate bypass" standard for procedural default),[44] and federal funds—say for additional custodial corrections expenditures—could be withheld.

As Professor James Liebman once wrote about capital cases: "[T]he logical cure for an error-prone system that chronically cycles products from a shoddy fabrication process to a long, expensive inspection process and back again is to devote more resources to the fabrication process in hopes that quality control eventually will require fewer resources."[45] We think it's best to pay now, and try to fix the problem at the front end, rather than waste our societal resources on inefficient and ineffective litigation at the back end.

That's the big picture. The details of such a reform proposal, of course, will be crucial to its success or failure. Although we have yet to work out these details, we can offer some preliminary thoughts about how some of them might look.

1. The State's Duty

In order to qualify for a new, leaner form of federal habeas review, Congress could require a state to meet clearly defined, federal standards for ensuring that

- all defendants, including indigent defendants, are provided quality defense representation;

---

[43] *See* Kent S. Scheidegger, *Habeas Corpus, Relitigation, and the Legislative Power*, 98 COLUM. L. REV. 888, 944 (1998) ("The point at which additional review is no longer producing a sufficient net increase in accuracy to justify its cost and delay is a policy question, and policy questions belong to Congress.").

[44] *See* LAFAVE ET AL., *supra* note 4, at § 28.4.

[45] James S. Liebman, *Opting for Real Death Penalty Reform*, 63 OHIO ST. L.J. 315, 326 (2002).

- all exculpatory evidence that is material is made available to defense counsel before trial or the entry of a guilty plea (e.g., by implementing police and prosecutorial "open file" policies);[46] and
- all post-trial claims of new evidence of factual innocence receive meaningful review, are investigated where necessary, and are referred to the state courts for remedial action where appropriate. This could be achieved through either (1) an open-ended opportunity for convicted defendants to present *new* evidence of factual innocence in state post-conviction proceedings or (2) an opportunity for review by an "innocence commission"[47] with the authority and resources to review and investigate claims of factual innocence made by convicted defendants and to refer cases involving such claims of factual innocence to the state courts for remedial action where appropriate. [48]

Under this radically shifted system, case-by-case adjudication about the trial, plea, or appellate performance of individual attorneys in non-capital cases would end. Neither

---

[46] *E.g.*, GOULD, *supra* note 30, at 190-93 (recommending open-file discovery as a response to wrongful convictions).

[47] One model might be the Innocence Inquiry Commission recently established in North Carolina. Patterned after the review of claims of innocence in the United Kingdom, the commission's members are appointed by the Chief Judge and must include a judge, prosecutor, victim advocate, defense attorney, sheriff, and member of the public, plus two other members. Claims of innocence would be screened by Commission staff and require new evidence not previously considered. The defendant must waive all privileges and agree to cooperate. The commission has independent investigative authority, including subpoena power. If the Commission finds there is sufficient evidence to merit judicial review, the case is referred to a three judge panel that, in turn, has the power to dismiss charges or find the defendant has not proven innocence. Jerome M. Maiatico, *All Eyes on Us: A Comparative Critique of the North Carolina Innocence Inquiry Commission*, 56 DUKE L.J. 1345, 1354-60 (2007).

[48] We also assume that states will continue to provide some judicial review of claims of illegal custody that do not question the validity of conviction or sentence: parole and goodtime violations, claims of sentence miscalculation, unconstitutional or illegal civil commitment under mental health or sexual predator laws, unlawful confinement prior to trial, etc. But these questions are handled in most states, we think appropriately, under procedures that are separate from those authorized for prisoners who file state post-conviction petitions challenging convictions and sentences.

state nor federal courts would consider claims of ineffective assistance. Instead, enforcement of federal standards could take several forms, so long as it occurs state-wide, and is not litigated on a case-by-case basis. For example, a state agency could regulate the certification and appointment of counsel in criminal cases in its state, following a number of standards promulgated by Congress. Or a federal agency could take on more of the oversight functions. Either way, ensuring ongoing state compliance could be part of federal agency oversight, with recourse to courts, to determine whether Congress's mandates have been carried out.[49]

This approach could do more to improve defense representation at the trial and appellate levels than *Strickland* ever could because effective representation would be ensured not by the unrealistic threat of post-conviction relief, but pervasively and systematically, without regard to the individual guilt of particular defendants, and impervious to waiver during negotiations.[50]

We do not presume to offer a definitive list of the requirements for the provision of adequate defense representation. Rather, Congress could draw upon the excellent and extensive research that already has been conducted in this area to craft individual standards or could charge a federal agency to do so. Some of the many ideas already proposed by

---

[49] The idea of prophylactic measures to prevent violations rather than case-by-case litigation over whether reversal is warranted as a remedy also has a storied history. Prior to *Strickland* scholars and courts argued that "preventative measures" such as improved training offered the primary route to achieving competent attorney performance. In an earlier time, the Court, fed up with case-by-case post-conviction review of custodial interrogations, substituted *Miranda* warnings and waivers. And few critics today bemoan the inability to overcome in post-conviction proceedings, the presumption of intelligence and voluntariness of each and every guilty plea that attaches upon compliance with certain prophylactic rules and standards that apply before the plea is accepted. *E.g.*, FED. R. CRIM. P. 11.

[50] Nancy J. King, *Regulating Settlement: What Is Left Of The Rule Of Law In The Criminal Process?* 56 DEPAUL L. REV. 389, 399 (2007) (arguing that "revisions in the resources allocated to public defenders' offices—changes that are not subject to waiver by the parties—may have a greater impact than tinkering with the postconviction rules governing ineffective assistance claims.").

the ABA, adopted by some states, or both include the following:[51] (1) a statewide mechanism for oversight, such as a state agency, independent of the state judiciary and not dependent upon county funding, with the mission, legal authority, and adequate resources provided by the state to oversee the provision of high-quality defense representation in that state; (2) minimum qualifications for defense counsel; (3) a process for the initial certification and recertification of defense counsel; (4) caseload limits;[52] (5) peer review of the counsel performance;[53] and (6) data collection of all complaints, peer reviews, and case results for individual attorneys[54] that the oversight body could review

---

[51] *See* LAFAVE ET AL., *supra* note 4, at § 1.4 nn.113-126 (collecting sources). *See also* UNITED STATES DEPARTMENT OF JUSTICE, CONTRACTING FOR INDIGENT DEFENSE SERVICES, http://www.ncjrs.gov/pdffiles1/bja/181160.pdf; THE STANDING COMMITTEE ON LEGAL AID AND INDIGENT DEFENDANTS, ABA TEN PRINCIPLES OF A PUBLIC DEFENSE DELIVERY SYSTEM (2002), http://www.abanet.org/legalservices/downloads/sclaid/indigentdefense/tenprinciplesbooklet.pdf.

[52] *See* BUREAU OF JUSTICE ASSISTANCE, KEEPING DEFENDER WORKLOADS MANAGEABLE (2001), http://www.ncjs.gov/pdffiles/bja/185632.pdf.

[53] *See, e.g.,* THE STANDING COMMITTEE ON LEGAL AID AND INDIGENT DEFENDANTS, *supra* note 50 (collecting performance standards). Our proposal would require each state to set up a system of meaningful peer review that would apply to both appointed and retained defense counsel. Without trying to prejudge the most appropriate specific features of such a system in every jurisdiction, we would anticipate a system that relies on a statewide Peer Review Committee composed of highly competent, deeply committed defense lawyers (e.g., the best of the state's public defenders). This committee would be given the primary responsibility to oversee defense counsel performance throughout the state. The committee would set and apply the standards of education, training, and experience for certification of defense lawyers, and would also ensure the integrity of the state's process for appointing defense counsel for indigent defendants.

[54] This empirical evidence could include information about the outcomes of trials and plea proceedings involving each defense lawyer and complaints filed by defendants against their defense lawyers. With the help of such a database, the overseers would be in a position to look for patterns of substandard outcomes and defendant complaints that would tend to show that a particular defense lawyer perhaps should be investigated.

Prior initiatives to collect data about the performance of criminal defense attorneys has tended to focus on aggregate data, which can be used to analyze systemic problems with defense representation systems, but which would be of limited use in assessing individual performance. *See, e.g.*, THE SPANGENBERG GROUP, INDIGENT DEFENSE STUDIES, http://www.spangenberggroup.com/work_indig.html; Letter from David J. Carroll, Director to the Michigan Supreme Court, http://www.sado.org/publicdefense/carroll_2005-09-27.pdf (proposing expanded data collection on performance of Michigan criminal defense attorneys).

as part of the recertification process.[55]

2. What's in It for the States: The Trade-Off

There are three potential sources of funding for this improved system of assuring that the constitutional rights of those accused of crime are honored. The first two sources are resources currently devoted to post-conviction litigation.[56] Institutionalizing competent counsel in the trial court and on direct appeal, open-file discovery, and innocence review will largely dispense with the need to maintain the kind of complex post-conviction apparatus that we currently have. It should be possible to shift significant resources from the "back end" of the criminal justice system to the "front end," where those resources can do more good. This shift could occur in three separate ways:

First, states that provide reliable and robust defense representation at the trial and direct appeal for every criminal defendant could decide to eliminate post-conviction review of criminal judgments in the state courts entirely, except for

---

[55] De-certification would not necessarily provide any ground for relief for defendants who had previously been represented by that lawyer (although a state could choose to provide a remedy for such defendants). Instead, such defendants would still have to satisfy, in federal habeas, the same standards as all other defendants, including the requirement of demonstrating likely innocence. But de-certification would at least ensure that no future defendants would suffer bad outcomes as a result of that lawyer's failings.

[56] The idea of trading aspects of federal habeas review for better defense representation earlier is not new to habeas commentary. Professor Daniel Meltzer raised the possibility at the end of an article criticizing the limitations of habeas review in 1993. Daniel J. Meltzer, *Habeas Corpus Jurisdiction: The Limits of Models*, 66 S. CAL. L. REV. 2507, 2526-27 (1993). Justice Powell's commission recommended over eighteen years ago that federal review be scaled back in return for better state post-conviction counsel in death cases, and a version of this opt-in scheme was endorsed by Congress, but these particular provisions have yet to be implemented. *See* Liebman, *supra* note 44, at 333. Also in death cases, Professor James Leibman recommended in the Ohio State Law Journal six years ago, for many of the same reasons we outline today, that in exchange for better counsel at the trial level defendants should *waive* post-conviction review. *See* Liebman, *supra* note 44, at 337. Unlike these earlier proposals, the suggestion floated here would have Congress *deny* federal habeas as we know it to defendants from states that meet these standards, and give states even more incentive and capacity to meet these standards by encouraging them to scale back their own state post-conviction review.

innocence review.[57]

Second, in return for providing better representation and discovery earlier in the process, the states would also enjoy a drastically cheaper *federal* habeas litigation bill. Congress could scale back federal habeas relief in these states. Rather than litigating, over and over again, thousands of meritless claims that are unrelated to innocence, states could target their post-conviction resources to only those cases remaining cognizable: those with promising claims of innocence of conviction or those involving retroactive application of a new rule. This change in the scope of habeas relief would slash the workloads of federal courts and states attorneys that now respond to habeas petitions. In many jurisdictions the money spent to provide post-conviction review (and defend post-conviction cases) may come from a different pot, so to speak, than funding for indigent defense. This will pose a political challenge for those advocating reallocation of these moneys—from the state's budget to a county or metropolitan budget or vice versa.

A third revenue source may be needed because the cost of providing adequate counsel to all of those facing felony charges probably dwarfs, in most states, the present cost of post-conviction review for those locked up long enough to seek it. That third source might be federal funds—which would assist and incentivize states to meet their Sixth Amendment obligations. Some federal funding could be reclaimed from the savings from scaling back federal post-conviction review, but we anticipate additional funds would be required both to set up the standards system and create enforcement mechanisms. Direct financial incentives for states that continue to demonstrate compliance with the higher standards could take many forms, including matching funds or conditioning related federal funding (say, for new prison beds, for example) on the provision of adequate defense statewide.

---

[57] Because federal habeas review of almost all claims will be conditioned on a showing of "clear and convincing evidence" of factual innocence, there will be no reason for defense counsel ever to "sandbag," or otherwise deliberately default a claim.

3. Letting Go of *Strickland* and *Brady*

Abandoning case-by-case post-conviction litigation in favor of prophylactic safeguards would mean that some very tiny fraction of defendants, who under the present system might have won the habeas lottery, would lose out. It is true that even under this tentative scheme, defense representation will never be perfect, and some clients will indeed pay for attorney errors if they have no convincing new evidence of innocence. Someone could spend his life in prison because his lawyer failed to file a suppression motion, when in another identical case, for example, where the lawyer did not make such a mistake, the defendant may go free. This is undoubtedly the most controversial part of our proposed rethinking of post-conviction relief. Yet if shutting down case-by-case litigation of such claims will help to provide *better* protection for *more* defendants, it is well worth the trade-off. The net result should be fewer instances of error overall, and that's exactly what the federal constitutional regulation of state criminal justice should produce.[58]

Post-conviction litigation presently works for too few, and too rarely, to provide deterrence of future violations. Abandoning these ineffective yet expensive tools would provide needed funds to furnish better counsel and information for far more defendants. Instead of the occasional person receiving a new trial or sentencing after a finding of ineffective assistance as the only check on state's failure to provide good lawyers, the new system would regulate counsel at the front end, through institutional sanctions that do not depend upon a defendant's ability to show that the errors of his counsel were so bad and the states' case against him so weak, that he deserves a new trial.

---

[58] Although we believe a radically shifted system would protect the right to counsel better than *Strickland* claims do now, states may choose to reap the benefits of reduced federal review and meet federal indigent defense standards while still preserving a case-by-case remedy for attorney failings. This would mean fewer freed-up state funds to provide for trial and appellate defense services. If a state did preserve review of IAC claims in state court, however, we would recommend implementation of a mechanism for speedy factual development of non-record claims in a motion for new trial or during appeal so that the appellate process could provide review of all claims (including IAC) *with an attorney* in *less time* than a subsequent post-conviction proceeding. *See* Primus, *supra* note 27 (recommending a unified appellate process including IAC claims).

Overall, more defendants should receive better assistance in more cases.

III. CAPITAL CASES

Although the focus of this presentation is the review of non-capital cases, the review of capital cases deserves mention. One of the main problems with current habeas law is that it is built almost entirely in response to concerns about the post-conviction review of the small number capital habeas petitions filed in federal court each year, ignoring the over 18,000 non-capital filings.[59] The problems in capital cases are specialized, and the two types of cases need not be addressed in the same way. Already many states have entirely different procedures for death penalty cases, and we believe it makes sense to follow this dual pattern in proposing any post-conviction reform.[60]

IV. CONCLUSION

Encouraging the states to concentrate their scarce criminal justice resources on improving defense representation, and freeing them from post-conviction litigation, will simultaneously address two of the most persistent problems in the criminal justice system today: the inadequate delivery of defense services,

---

[59] *See* JAMES C. DUFF, ADMINSTRATIVE OFFICE OF THE U.S. COURT, JUDICIAL BUSINESS OF THE U.S. COURTS, 145-47 tbl.C-2, http://www.uscourts.gov/judbus2007/appendices/C02Sep07.pdf.

[60] At the least, we would suggest that if a similar trade-off is considered for capital cases, federal habeas review should remain available in more circumstances than we suggest for non-capital cases. *See generally* Joseph L. Hoffmann & William J. Stuntz, *Habeas After the Revolution*, 1993 SUP. CT. REV. 65 (1994) (arguing for concept of "two-track" federal habeas). Merits review should be preserved not only to those defendants who can make a "clear and convincing" showing of factual innocence or to those who are entitled to the retroactive application of new rules (as in non-capital cases) but also to those who demonstrate that the aggravating circumstance on which the death sentence was premised was not adequately proven (i.e., "actual innocence" of the sentence), or that the death sentence is an unconstitutional penalty in light of the defendant's crime, *see, e.g.,* Kennedy v. Louisiana, 128 S. Ct. 2641 (2008) (unconstitutional to impose death penalty for rape of child when victim is not killed), or status, *see, e.g.,* Atkins v. Virginia, 536 U.S. 304 (2002) (unconstitutional to impose death penalty for crime committed by mentally retarded defendant); Ford v. Wainwright, 477 U.S. 399 (1986) (unconstitutional to execute defendant who is insane).

and the years and years of wasteful and misdirected litigation after appeal.

Of course, this represents a kind of compromise, and compromises tend to make nobody happy and everybody suspicious. States may argue that federal standards for defense representation go well beyond existing constitutional mandates for the right to counsel, that Congress has no business conditioning federal remedies on state policy choices, or that money saved by reducing state and federal post-conviction review could be more wisely spent on something other than padding the pockets of criminal defense attorneys. Defense advocates, including many of our own academic colleagues, may complain that scaling back of already meager post-conviction remedies for serious violations of constitutional rights, particularly the right to effective assistance of counsel, will result in even more constitutional violations and wrongful convictions. More post-conviction review of the merits of claims, not less, they may argue, is needed.

We think that both of these positions are shortsighted and that Congress and state governments together can do a better job providing the procedures mandated by the Constitution without bankrupting the states. Whether one's metric is accuracy or constitutional compliance, any meaningful shift of resources from the post-conviction review now in place to defense representation earlier in the process would be an improvement over what we have today. Certainly the number of defendants who could use better lawyers before conviction far exceeds the number of defendants that might be harmed by eliminating existing post-conviction litigation after appeal, especially when review is retained for convincing claims of innocence.

The triple-layered, expensive process of state and federal review of criminal judgments now in place was constructed during a historical period when federal judges were at odds with state judges in criminal cases, when a smaller proportion of our population was sentenced to lengthy prison terms, and when DNA testing had yet to reveal how those innocent of crime could be found guilty. It is time to consider whether the structure

built upon the outdated assumptions of this earlier era has outlived its usefulness. We believe that it has, and that post-conviction policy should take a new direction. The most formidable barrier to the enforcement of the Constitution is not the state judiciary; it is inertia.

PUTTING OUR EXPERTISE
INTO PRACTICE.

WS&T

WILKINS, STEPHENS & TIPTON, P.A.
ATTORNEYS AT LAW

Offices In Jackson, MS (601-366-4343), Greenville, MS (662-335-5555)
and Nashville, TN (615-661-7820) • www.wilkins-law.com

© 2008 Wilkins, Stephens & Tipton, P.A. All rights reserved.

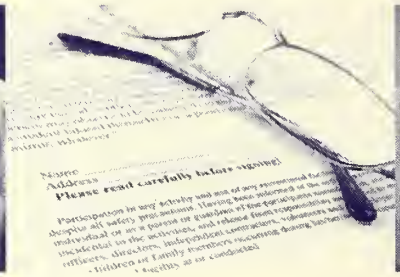
Select from over 20 pieces of Electronic Reference Literature
at ***www.lexisnexis.com/lawschool***

LexisNexis®

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Inc., used under license.
© 2008 LexisNexis, a division of Reed Elsevier Inc. All rights reserved. LA12712-0 1008

Mississippi Briefing Service

...an indispensable service provided by the... Mississippi Law Journal



In the legal world, timely and accurate ***communication*** *is a key to* ***success...***

How can you stay informed of the latest appellate decisions without sacrificing your valuable time?

Answer: the Mississippi Briefing Service

Each week, *Recent Decisions of the Mississippi Supreme Court and Court of Appeals* briefs the latest opinions of the Courts. In addition to concise and accurate summaries, each case is supplemented with appropriate and accurate headnotes—which means you find the cases you need and only the cases you need.

Annual subscription to the Mississippi Briefing Service is available for $85 and is provided in searchable, electronic format via e-mail, providing you the information you need even faster.

To subscribe, or for a free sample brief:

- e-mail: **MSBRIEF@OLEMISS.EDU**
- write: Mississippi Law Journal
  P.O. Box 849
  University, Mississippi 38677

Mississippi Law Journal
student-operated, student-lead, practitioner-focused